UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS INFORMÁTICOS

TEMA: DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

AUTOR: GALO PATRICIO ALOMOTO CUVI

TUTOR: MG. CHRISTIAN PATRICIO VACA BENALCÁZAR CPA

QUITO - ECUADOR

AÑO: 2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA UNIDAD EDUCATIVA ADVENTISTA GEDEÓN", ha sido desarrollado por el señor Galo Patricio Alomoto Cuvi con C.C. No. 1715967459 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Galo Patricio Alomoto Cuvi

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA UNIDAD EDUCATIVA ADVENTISTA GEDEÓN", presentado por Galo Patricio Alomoto Cuvi, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M., 16 de agosto de 2019

TUTOR

Mg. Christian Patricio Vaca Benalcázar CPA

AGRADECIMIENTOS

Me gustaría agradecer en estas líneas la ayuda que mi novia Ibeth Cedeño me ha prestado durante el proceso de investigación y redacción de este trabajo.

Así mismo, quiero agradecer a mis padres que me han ayudado y apoyado en todo mi producto, a mi tutor, Ing. Christian Vaca, por haberme orientado en todos los momentos que necesité sus consejos.

A todos mis amigos, vecinos y futuros colegas que me ayudaron de una manera desinteresada, gracias infinitas por toda su ayuda y buena voluntad.

A la Universidad Tecnológica Israel por ser la sede de todo el conocimiento adquirido en estos años

DEDICATORIA

Esta tesis está dedicada a mi padre Galo, quien me enseñó que el mejor conocimiento que se puede tener es el que se aprende por sí mismo.

A mi madre Elsa, quien me enseñó que incluso la tarea más grande se puede lograr si se hace un paso a la vez.

A mis hermanos Lenin e Isaac por el apoyo moral, que me brindaron a lo largo de esta etapa de mi vida.

A mi novia Ibeth, por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias.

A mi hija Thais, por ser quien dibuja la sonrisa en mi rostro.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

La variedad actual de dispositivos informáticos y el creciente desarrollo de habilidades en esta área, además de la importancia en materia económica que representa el manejo de la información para las empresas, hacen que la seguridad informática se convierta en un tema constantemente actualizado. La Seguridad de la Información (SI), concebida desde una perspectiva global, no está circunscrita exclusivamente al resguardo físico de los documentos, sino que engloba a todos los activos informáticos con los cuales se crean y transmiten estos, además de las personas que tienen acceso a la respectiva información, de esta manera la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es siempre necesaria. El objetivo fue diseñar una propuesta de SGSI para la Unidad Educativa Adventista Gedeón, fundamentado en la norma ISO 27001:2013. Para esto, se realizó un inventario general, así como una valoración del nivel de cumplimiento de los requisitos establecidos en dicha norma, en base a estos resultados, se generaron propuestas de acciones y correctivos mostrados en la estructura documental propuesto por la normativa empleada. Se observó un alto nivel de incumplimiento con la normativa, en un 79,89% de los casos no se cumplen los requisitos del Anexo A de la norma ISO, ni en 86,1% de las veces con las disposiciones de los apartados 4 al 10 de esta. Se concluye que la institución es altamente vulnerable en términos de la SI y que debe lo más pronto posible implementar el SGSI que se propone.

PALABRAS CLAVES: Propuesta, Sistema, Gestión, Seguridad, Información, Educación, ISO.

ABSTRACT

The current variety of computing devices and the growing development of skills in this area, in addition to the importance in economic matters that information management represents for companies, make computer security a constantly updated topic. Information security, conceived from a global perspective, is not limited exclusively to the physical protection of documents, but includes all the computer assets with which they are created and transmitted, in addition to the people who have access to the respective information, in this way the implementation of an Information Security Management System (ISMS) is always necessary. The objective was to design an ISMS proposal for the Gedeon Adventist Educational Unit, based on the ISO 27001: 2013 standard. For this, a general inventory was carried out, as well as an assessment of the level of compliance with the requirements established in said standard, based on these results, proposals for actions and corrective actions were shown in the document structure proposed by the regulations used. A high level of non-compliance with the regulations was observed, in 79.89% of the cases the requirements of Annex A of the ISO standard are not met, nor in 86.1% of the time with the provisions of sections 4 to 10 of this. It is concluded that the institution is highly vulnerable in terms of information security and that it should as soon as possible implement the proposed ISMS.

KEYWORDS: Proposal, System, Management, Security, Information, Education, ISO.

INTRODUCCIÓN

Antecedentes

La Unidad Educativa Adventista Gedeón es una institución de carácter privado que está dedica a formar niños, niñas y adolescentes a nivel de Educación General Básica y Bachillerato. Tiene como misión, brinda una educación basada en valores y principios cristianos que busca una transformación del proceso enseñanza - aprendizaje dentro del aula escolar. Actualmente, se encuentra ubicada en el sector de la Armenia de la ciudad de Quito en la calle Charles Darwin Lote 244 y Vicente Solano y es parte de las 24 instituciones de educación adventista.

En esta institución educativa, no se dispone de políticas, normas y procedimientos que orienten a los empleados sobre cómo mantener mejores prácticas para salvaguardar la información que se genera o resguarda en la institución.

Además, existe una falta de conocimiento de los mecanismos tecnológicos que resguarden la información, así como también de las tendencias tecnológicas para protegerse contra amenazas y ataques tanto internos como externos a la institución y de esta manera evitar eventos que pongan en riesgo su patrimonio digital por medio de violaciones informáticas.

Así mismo, presenta potenciales amenazas relacionadas con elementos internos y externos a la institución debido a la no implementación de estrategias y mecanismos que normalicen y controles a los activos de la información que posee.

La misma, es parte de la Red Adventista de Educación, la cual, es subvencionada por la Iglesia Adventista del Séptimo Día, la cual, "*se encuentra presente en más de 150*

países con aproximadamente 1.5 millones de alumnos [y] solo en América del sur cuenta con más de 500 unidades escolares que ofrecen desde educación básica a postgrados, incluyendo colegios con residencias estudiantiles" (Unidad Educativa Adventista Gedeón, 2019).

Como otras unidades educativas de carácter religioso, entre las actividades académicas normales, promueven un sistema educativo basado en principios cristianos, propios de los practicados por los seguidores adventistas. En resumen, la Unidad Educativa Adventista "Gedeón", es una institución educativa, interconectada a una red educacional de carácter nacional e internacional, que cuanta con un grupo de 31 empleados y una base de estudiantes de 350 niños y jóvenes, distribuidos desde primaria a bachillerato.

Planteamiento del problema

A nivel mundial, la inclusión de un Sistema de Gestión de Seguridad de la Información (SGSI) ha permitido "*evitar el mal uso, abuso y hurto de información organizacional en 73%*" (Ríos, 2018, pág. 96). Ante esto, países como los Estados Unidos, consideran que es "*de amplia relevancia a nivel jurídico digital que las empresas garanticen sus protocolos informáticos con normativas de regulación y control por medio de las Normas ISO*" (Hunter Control Systems, 2019, pág. 82).

El SGSI en las organizaciones permite evitar las actividades malintencionadas cuyo objetivo es causar daño como: robar o destruir información, incitar colapsos del sistema, rechazar servicios, etc. Ante esto, el alcance que tiene hoy la tecnología "*impide la vulnerabilidad de cualquier sistema y resulta imprescindible mantener un medio protegido con un nivel de seguridad lo más elevado posible garantizando los procesos institucionales a corto y largo plazo*" (Valverde, 2017, pág. 77).

En Latinoamérica, de acuerdo a un estudio privado con fines investigativos por Castro y Jácome (2017) existen "*cerca de 427 medianas y grandes empresas que mantienen como forma de protección de sus sistemas de información la inclusión de la Norma ISO 27001*" (p. 251). Así, se garantizan que los procesos sean estandarizados, regulados y controlados por las instituciones que se acogen a dicha normativa.

Sin embargo, en Ecuador, la gestión de los riesgos y la seguridad de los activos informáticos, son áreas fundamentales que en poco nivel se han estudiado a pesar de ser dos de los principales puntos a tomar en cuenta dentro de cualquier institución en la que se maneje un sistema informático y en la que se mantenga información clave de sus usuarios (Encalada, 2017, pág. 81).

Actualmente, en el afán de aprovechar dichas falencias, de forma constante se desarrollan nuevos métodos que afectan la seguridad de la información (SI); por lo cual, se requiere realizar un estudio de dichas amenazas y definir un SGSI que minimice los riesgos asociados "*al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada, minimizando así el porcentaje de riesgo y pérdida de datos*" (Fonseca, 2017, pág. 81).

A nivel de las instituciones educativas nacionales, estas manejan información sumamente importante como son los datos académicos de cada uno de los estudiantes. Por tal motivo, "*se hace indispensable que un SGSI genere confidencialidad, integridad y disponibilidad*" (Benavides, 2018, pág. 14).

En Ecuador, la educación adventista, fundamentada en el apoyo de la Red Adventista Internacional, comenzó sus labores docentes en el año 1968, y hasta la fecha, se ha expandido desde la educación inicial básica hasta la universitaria.

En la unidad educativa no existe alguna persona encargada del control de los sistemas informáticos y a la presente fecha, ésta no cuenta con ningún estándar implementado, únicamente toma ciertas medidas preventivas las cuales no garantizan la correcta gestión y SI, por lo que personas o entidades mal intencionadas podrían tener acceso a datos que se manejan internamente y hacer uso inadecuado de los mismos.

A pesar de ser una unidad educativa pequeña comparada con otras instituciones adventistas del país, la cantidad de estudiantes es significativa por lo que constantemente se genera un gran flujo de información. La necesaria interconexión con la red educativa adventista tanto nacional como internacional, también implica el constante manejo de recursos informáticos que permitan garantizar la misma.

En este sentido, y considerando el contexto y las interacciones institucionales y personales antes mencionadas, se enumera a continuación una lista de las situaciones que pueden considerarse como parte del problema de estudio:

- Falta de protocolos de manejo y controles de los activos de la información.
- Inexistencia de mecanismos para el control de ingreso a las áreas donde se maneja información sensible.
- Falta de resguardo de los activos de la información tanto físicos como lógicos.
- No existe un SGSI
- La institución carece de un sistema de evaluación de activos de la información

Para la protección de dicha información es necesario que la institución se acople a las Normas ISO 27001, cuyos estándares permiten originar un conjunto de pautas concernientes a la gestión de los mecanismos de seguridad, haciendo énfasis en tres aspectos: disponibilidad de la información, confidencialidad, e integridad de esta y que los mismos den una estabilidad y garantía informática a la Unidad Educativa Adventista Gedeón. Todo esto debido a que, como se mencionó, no existen procedimientos estándares para el manejo de la información, lo cual incluye, carencia de bases sólidas de seguridad, privacidad y acceso, existiendo de esta manera la posibilidad de que en determinadas situaciones, esta, pueda estar expuesta a terceros, y pueda perderse, tanto por situaciones catastróficas como por negligencia y mala intención.

Justificación

La información académica es un recurso clave para el Ministerio de Educación ecuatoriano, por tal razón se debe gestionar de manera eficiente la seguridad de la misma (Ministerio de Educación ecuatoriano, 2019), más aun, cuando dentro del entorno nacional han aparecido graves amenazas de modificaciones de expedientes académicos en los sistemas informáticos, con lo cual es posible la existencia potencial del riesgo de que la información educativa sea robada o usada inapropiadamente.

Ante esto, la propuesta de un SGSI construido en base a la Norma ISO 27001 permitirá de manera substancial el adecuado manejo y gestión de la información en la

Unidad Educativa Adventista Gedeón, misma que no cuenta con una metodología de gestión adecuada de la información.

La inclusión de la Norma ISO 27001 tiene como objetivo crear una estructura de la SI para la institución, además de implementar controles, evaluaciones y tratamiento de riesgos, garantizando de esta manera el manejo y trato de los datos institucionales de sus estudiantes.

Los beneficios más relevantes a obtener por medio de la implementación del SGSI serán "integridad, confidencialidad y disponibilidad de la información" (Bermúdez & Bailón, 2015). Además, la correcta gestión de la misma producirá una serie de ventajas para la Unidad Educativa Adventista Gedeón debido a que "una administración adecuada y efectiva se traduce en mayor eficiencia de los procesos que se llevan a cabo, estabilizando al largo plazo sus funciones" (Varela, 2017, pág. 197).

La unidad educativa donde se desarrolló la presente investigación, maneja información sensible de alumnos y representantes, además, se pude interconectar con una red administrativa más amplia y externa a la institución, sin embargo, de manera explícita no existen controles para garantizar la SI o de sus activos, integrados a un SGSI con el cual se garantice operativamente la SI con que trabaja la institución.

El descontrol y la informalidad relacionada con la implementación de prácticas de seguridad para el resguardo de la información dentro de la unidad educativa, podrían repercutir en la perdida de información sensible o incluso, facilitar el acceso de tercero a la red institucional perdiéndose de esta manera "*la confidencialidad, disponibilidad e integridad de los activos de la información*" (Barrantes & Hugo, 2012; Jiménez, 2017).

Se requiere sea implementado un SGSI, que garanticen el control adecuado de todos los activos informáticos de la unidad educativa, de esta manera, se lograría disminuir los riesgos, haciendo que estos sean conocidos, contrarrestados de manera organizada por parte de la institución afectada tras el empleo de un plan adecuado para tal fin.

Por lo expuesto anteriormente, se justifica el desarrollo del presente proyecto, el mismo que de ser aplicado en la institución de estudio ofrecerá un aporte de suma calidad para el servicio que ofrece a la ciudadanía.

Objetivos

Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la Información para la UE Adventista Gedeón mediante la aplicación de la norma internacional ISO/IEC 27001:2013 que incluya directrices, normativas, políticas y controles aplicables al mejoramiento de los estándares de seguridad informática en la institución.

Objetivos específicos

- Analizar la situación actual de la UE Adventista Gedeón por medio de un GAP Análisis (análisis de brecha).
- Comprobar las vulnerabilidades y debilidades de los mecanismos de control de los activos informáticos de la UE Adventista Gedeón.
- Definir los controles basados en el Anexo A de la norma ISO 27001, que aplican a la UE Adventista Gedeón como la propuesta para las políticas de SI.

Debido al carácter técnico y de implementación que caracteriza a la presente investigación, no es aplicable el planteamiento de un sistema de hipótesis. En este estudio, no se pretende comprobar ningún fenómeno u experimento, ni verificar la interacción de elementos asociados al tema, por lo que, no es necesario el planteamiento de hipótesis. Por el contrario, este trabajo se sustenta en la realidad comprobable del riesgo que en la actualidad puede padecer una institución cualquiera al no poseer los adecuados mecanismos para salvaguardar sus activos informáticos, en este sentido, el estudio parte de determinar el nivel de implementación de controles pertinentes asociados al tema, pasa por verificar vulnerabilidades y en base a esto, proponer un SGSI.

Descripción de los capítulos

La estructura capitular de la investigación está conformada de la siguiente forma:

Capítulo I: Fundamentación teórica, hace referencia a todos los elementos teórico – conceptuales que se van a manejar dentro de la problemática expuesta partiendo del estado del arte, la información institucional, los elementos técnicos a utilizar y la información de las potenciales soluciones.

Capítulo II: Marco metodológico, determina los procedimientos científicos para dar solución a la problemática y que están compuestos por el tipo de investigación, la recopilación y técnicas de información, tabulación y análisis de resultados.

Capítulo III: Propuesta, describe el diagnóstico de la situacional actual realizado, la factibilidad en los ámbitos técnico, operacional y económico del modelo generado con lo cual se genera el sustento de trabajo para la generación en detalle de una propuesta de SGSI fundamentado en la Normativa ISO 27001 y adaptado a las necesidades de la institución.

Capítulo IV: Implementación, en esta sección se describe en detalle el documento técnico que dirige de manera definitiva las características y generalidades del SGSI que se propone.

CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA

1.1. Estado del arte

A nivel de Latinoamérica ni del mundo existe una totalización específica para unidades educativas que hubieran implementado SGSI basados en la Norma ISO 27001, sin embargo, si se puede acceder a unas estadísticas empresariales globales, mismas que para el 2015 “México lideraba con 104 certificados, seguido de Colombia con 103, Brasil con 94, Argentina con 52, Chile 32, Perú 22 y Uruguay 21” (2018, pág. 36); datos que se puede validar en la figura 1.1:

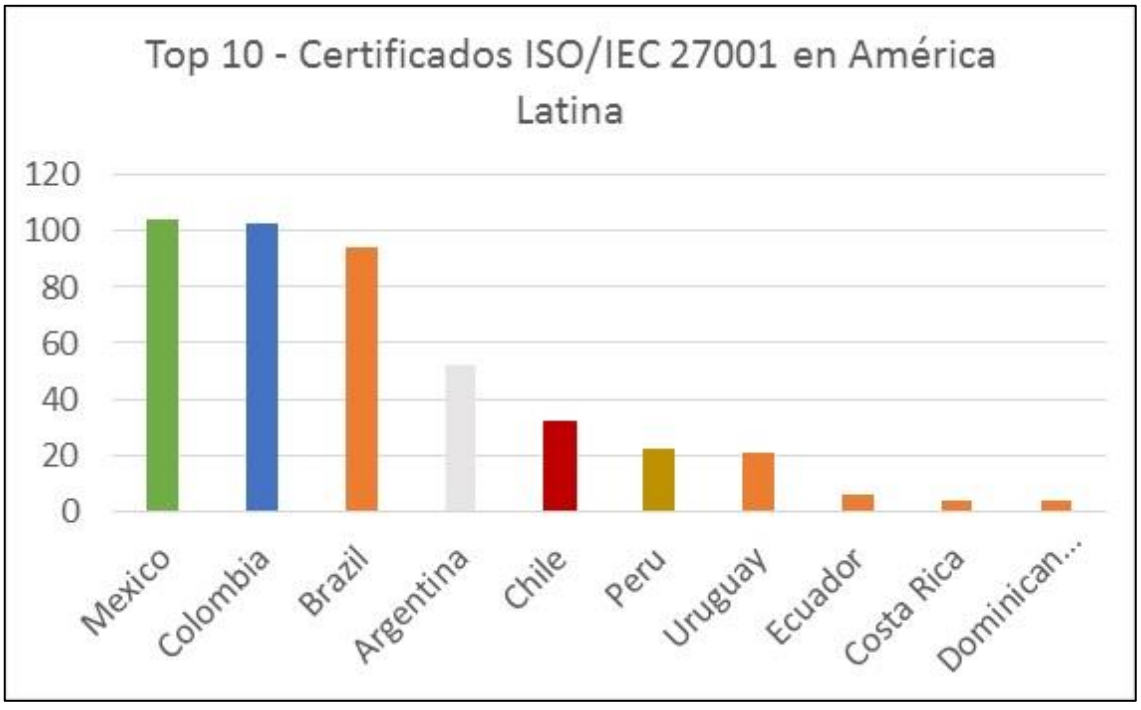


Figura 1.1 Top 10 por países de empresas con certificados de la Norma ISO 27001. Fuente: Datasec (2018)

Sin embargo, desde la fecha en que se publicaron estos valores, según lo expone Datasec (2018), las cantidades de empresas certificadas con la Norma ISO 27001, en

países como México y Colombia, ha incrementado de manera considerable (Tabla 1.1), por su parte, en Brasil su desarrollo ha sido mínimo; pero en Argentina y Ecuador dichas certificaciones han decrecido, según el análisis de Crespo (2018) este decrecimiento "se debe a claros procesos recesivos que afectan las economías nacionales y reducen la brecha productiva de las empresas" (pág. 22).

Tabla 1.1. ***Desarrollo histórico de empresas latinoamericanas con certificado ISO 27001***

País	**Año**			
	2015	2016	2017	2018
México	104	221	315	421
Colombia	103	163	148	179
Brasil	94	117	170	189
Argentina	52	88	57	21
Ecuador	6	11	8	5

Fuente: Datasec (2018)

Los datos referenciados, comprueban que Ecuador es uno de los países con menor dinámica empresarial en asumir la certificación de la Norma ISO 27001. Dentro del contexto nacional, existen varias investigaciones que hacen referencia al SGSI sustentado en la Norma ISO 27001 y su aplicación en empresas de diferentes áreas como, por ejemplo, a nivel militar, farmacéutico, sector público (gubernamentales) y educativo, entre estas se encuentran las que a continuación se describen.

Guamán (2015), realizó un trabajo titulado: "Diseño de un SGSI para instituciones militares aplicado al COAAS, COBAS y FAE", en este, se expone que "las instituciones militares ecuatorianas, actualmente no disponen de un SGSI para resguardar los activos de información que poseen, lo que dificulta mantener la información de acuerdo a las normas de la norma ISO 27001" (pág. 184).

Es pertinente mencionar que al 2019, no existe mayor novedad sobre las repercusiones de esta investigación, determinando en forma general que la problemática aún puede ser existente dentro de las instituciones militares.

Además, Vallejo (2018) en el proyecto "Propuesta de SGSI para el centro de datos de la empresa Leterago del Ecuador S.A.", expresa que la Norma ISO 27001, permite identificar los riesgos existentes en los activos de información y la forma de mitigarlos,

más los controles que utilizan en la organización para evitar riesgos con esta información, logrando realizar políticas de SI y una propuesta de SGSI que permite a la organización disminuir los riegos a un nivel aceptable por lo tanto poder proteger las actividades que son esenciales en el giro del negocio (p. 129).

Bajo esta perspectiva, queda claro que la Norma ISO 27001 permite generar políticas de mejor manejo informático de la información al punto de re consolidar las actividades empresariales.

Por su parte, Bailón y Bermúdez (2015), en la investigación académica titulada *"Análisis de la seguridad informática y SI basado en la Norma ISO 27001 dirigido a empresas"*, concluyen en su investigación que "para minimizar los riesgos existentes, es pertinente implementar controles de seguridad, lo cual ayuda a robustecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información. Pero los resultados también muestran la importancia del compromiso y trabajo en equipo que debe tener siempre la empresa" (pág. 12).

El trabajo de Bailón y Bermúdez (*Ibid),* determina que, dentro de un SGSI, se debe mantener como meta institucional la confidencialidad, integridad y disponibilidad de la información y ese debe ser el camino que debe tener una propuesta.

Otro trabajo que se puede citar, es el realizado por Brito (2017), presentó un trabajo titulado "Los Sistemas de Gestión de Seguridad de Información en procesos de control para instituciones gubernamentales ecuatorianas", en este, formula que la información debe mantener siempre un proceso de seguridad informática en todas las instancias, fuera del costo que pueda representar, nada es más perjudicial que alguien se apodere de los datos de una organización, así cualquier medio que lo garantice no es un gasto sino una inversión (pág. 94).

El autor antes citado, valida entonces en su investigación que un SGSI fuera de su costo de implementación, es una clara inversión que toda organización debe ejecutar por salvaguardarse como empresa.

Por su parte, Palacios (2018) dentro del proyecto "Auditoría a la seguridad informática en la Dirección Distrital 02D03 Chimbo - San Miguel - Educación durante el período enero 2016 - octubre 2017, utilizando la norma internacional COBIT", indica que su investigación contribuyó significativamente a la resolución del problema que se planteó, proporcionando información sobre la adecuada gestión de riesgos informáticos, con el propósito de precautelar los activos más importantes y aportar en el cumplimiento de los objetivos institucionales (Palacios, 2018, pág. 18).

Por tanto, deja claro que la auditoria de seguridad es un estudio preliminar que debe emitirse antes de cualquier cambio profundo en la institución como acción previa a la instauración de una normativa de gestión.

Igualmente, el proyecto de tesis "Automatización del proceso de gestión académica de pre - básica del Instituto Educativo privado Children Genios y Noruega escuela" (Iza, 2018), expone que la implementación de esta aplicación web optimizó el método de calificación estudiantil, se redujo tiempos de generación de reportes y minimizó errores de asignación de calificaciones además de obtener información académica de los alumnos (*Ibid* p. 11).

Además, Bonilla (2018) a nivel de su proyecto "Diseño de un sistema de gestión de seguridad de información bajo la ISO 27000 para la Unidad Educativa particular Séneca", menciona que los beneficios de un SGSI son muchos, aunque no es implementado sino más bien un diseño, es una muestra de su eficacia al tratar con recursos tecnológicos y de información (*Ibid* p. 98).

Así, se determina que no es necesaria la implementación de la normativa del SGSI, sino que el estudio puede demostrar que a futuro las instituciones pueden instaurar la propuesta y obtener los beneficios identificados en el proyecto, dado que muchas veces requiere de una inversión económica que sobre pasa la realidad financiera de las instituciones.

En un entorno específico Ortiz (2017) en su aporte de tesis *"Sistemas de control y protección informática para unidades educativas del milenio, caso Quito 2017"*, manifiesta:

La mayoría de departamentos de las instituciones estudiadas a nivel informático no mantienen claros procesos de control y los problemas de seguridad, si bien son definidos se llegan a mantener hasta por 3 años seguidos sin soluciones del caso, por más que existan evaluaciones anuales (p. 108).

Así, el autor deja en claro que si bien se realizan propuestas de solución muchas de las veces no son aplicados y las problemáticas de seguridad se siguen manteniendo, donde uno de los aspectos de mayor limitación son los recursos económicos antes que los administrativos para instaurar aportes integrales.

Por su parte, Guevara (2017) en su aporte "SGSI basada en la Norma ISO 27001 para el departamento de tecnologías de la información y comunicación de las Unidades Educativas de Quito" cita:

Gracias a las diferentes restricciones y parámetros de seguridad de los sistemas institucionales, los archivos y documentos se encuentran correctamente respaldados y documentados. El problema radica en la falta de seguridad a la red interna convirtiéndose en blanco fácil ante ataques informáticos (p. 86).

Concluyendo, que una propuesta de SGSI para la Unidad Educativa Adventista Gedeón utilizando Normas ISO 27001, no sólo es viable sino eficiente y teóricamente su instauración tendrá un potencial éxito.

1.2. Lógica del negocio

1.2.1. Estructura organizacional

La institución tiene una estructura orgánica sencilla, constituida por un Rector, un Vice Rector, Un Director académico, un administrador, cuatro secretarias y 30 docentes.

1.2.2. Plan estratégico

La planeación estratégica de la institución, está compuesta por Misión, Visión y Valores, los cuales se muestran textualmente a continuación

- Misión y visión:

Promover una educación integral donde desarrollamos los valores, la mente y el cuerpo.

- Valores:

"*La Red de Educación Adventista basa su pedagogía en principios bíblicos-cristianos. Estos valores son aplicados en todas las vivencias académicas del estudiante. Para reforzar esa experiencia, la Red desarrolla el Plan Maestro de Desarrollo Espiritual (PMDE), que enfatiza, a cada bimestre, las virtudes que deben formar parte de la vida en sociedad, tales como: humildad; la igualdad; generosidad e integridad. Una formación completa, que considera al ser humano como manifestación del amor, cuidado y creación de Dios*" (Unidad Educativa Adventista Gedeón, 2019).

1.3. La seguridad de los activos de la información y los SGSI.

Las instituciones dependen cada vez más de sus SI que contienen y crean valor, y constantemente se recopilan y usan datos de clientes, los cuales son almacenados en bases de datos que pueden o no estar adecuadamente protegida y administradas, lo que permite garantizar su seguridad y evitar que sea sustraída y entre otras cosas, por ejemplo, empleada en marketing que el dueño de dicha información no quiere recibir (Martin, Borah, & Palmatier, 2017).

El objetivo de tener un SI seguro y confiable lleva a las organizaciones a implementar reglas de seguridad formalizadas en políticas de SI (ISP, por las siglas en inglés de: *Information Security Policies*). Esta política, define los requisitos de seguridad para todos los recursos (*hardware*, *software*, datos de información personal, procedimientos, procesos, etc.) tanto internos como externos (Cohard, 2019).

Cabe señalar que "*Se estima que para el año 2019 el costo total anual del delito cibernético en la economía mundial podría sobrepasar los 2 billones de dólares. El 70% de las empresas no tienen un plan de acción ante estos ataques*" (WTW, 2018). Este costo es adicional al daño de imagen que puede resultar de un "mal uso" de los datos, como en el caso del escándalo de *Cambridge Analytica* (BBC Mundo, 2018).

En este contexto complejo, la administración enfrenta varias amenazas que deben evaluarse. De hecho, las personas en la organización pueden ser factores de riesgo para el SI como por ejemplo: a través del incumplimiento de las políticas de seguridad, negligencia o falta de capacitación, por lo que la identificación de las fallas que afectan la capacidad de los empleados para cumplir con las recomendaciones de seguridad es fundamental (Gil & Gil, 2017).

Al respecto, Ortiz indica que "*la alta informatización de la sociedad moderna ha generado el incremento de los llamados 'delitos informáticos*" (2017, pág. 243), por lo que, sostiene que solamente serán seguros los sistemas informáticos que estén adaptados para cumplir la reglamentación de seguridad establecida en base al SGSI al que pertenecen.

Un SGSI se puede definir como el conjunto de políticas, actividades y recursos administrados colectivamente por una organización para proteger sus activos de información. Esta definición muestra claramente las diferentes dimensiones de este sistema, que consta de Tecnologías de la Información (TI), elementos personales y organizativos, así como de gestión (políticas, procedimientos) orientados a la defensa de los activos de la empresa, por lo que los enfoques propuestos por la norma para la implementación de un SGSI es el de los procesos (Cohard, 2019).

Ante esto, la seguridad en los sistemas informáticos está determinada como "un conjunto de soluciones técnicas, métodos y planes cuya meta es que la información tratada en los sistemas informáticos esté protegida y permita establecer un plan de seguridad dentro del cual se definan las necesidades y objetivos en cuestiones de seguridad" (Pedrosa, 2018, pág. 185).

Así es prioritario exponer que la seguridad tiene un determinado precio muy a expensas de que en la práctica es improbable alcanzar un nivel absoluto de seguridad, por lo que, para adaptar lo mejor posible las estrategias a seguir, deben evaluarse, primeramente, y de manera minuciosa, cual es la situación de la institución para lograr obtener un punto de partida adecuado y realista.

1.3.1. Importancia de la seguridad de la información

La importancia de la seguridad de la información (SI) radica en que está orientada en garantizar la protección contra las amenazas generadas por las vulnerabilidades de los activos de la información (Berumen & Arriaza, 2008).

La información representa para las empresas un elemento con elevada importancia que, además dependiendo del contexto en el que se basen estas informaciones, incluso puede generar perjuicios empresariales y personales si la misma es sustraída, eliminada o utilizada con fines delictivos. La Organización Internacional para la Normalización/International Engineering Consortium (ISO/IEC), confirma que los sistemas de información son de suma importancia y recomienda que esté siempre protegida adecuadamente (ISO, 2005, pág. 29).

En general, la SI es un requisito obligatorio para minimizar los riesgos asociados a una actividad o negocio y asegurar así la conformidad con las disposiciones legales o de carácter regulatorio, como es el caso de reglamentos comunitarios o procedentes de la legislación de algún país.

En Ecuador, desde el año 2013, se estableció el empleo obligatorio para los entes públicos de un Esquema Gubernamental de SI (EGSI) (SENPLANDES, 2013), en cual está fundamentado en la NTE INEN-ISO/IEC 27000 y se evalúa en base a la norma no certificable INEN ISO/IEC 27002.

1.3.2. Objetivos que persigue la seguridad de la información

Las propiedades que distinguen a la SI y por ende, a sus objetivos como método de seguridad son: autenticidad, confidencialidad, disponibilidad, identificación y control e integridad (Zambrano, 2018, pág. 76).

Por su parte, los objetivos de SI deben sujetarse bajo los siguientes lineamientos: "*identificación de los usuarios, detección de intrusos en la red, análisis de riesgo, clasificación apropiada de los datos, control de las nuevas aplicaciones, análisis de los accesos de los usuarios*" (2017, pág. 62), al respecto, se define a los mismos como se muestra en la Tabla 1.2:

Tabla 1.2***. Lineamientos que definen los objetivos de los SGSI***

Característica	Descripción
Identificación de los usuarios	Reconocer a quienes ingresan al sistema bajo un código de entrada (*password*)
Detección de intrusos en la red	Determinar al personal no autorizado que accede al sistema en tiempo real
Análisis de riesgo	Identificar las amenazas de seguridad, además del nivel de frecuencia con la que se producen dichas amenazas; reconociendo la protección contra las mismas y las pérdidas potenciales que se pudiesen generar
Clasificación apropiada de los datos	Se debe generar una buena supervisión de la seguridad ante los diferentes datos que van ingresando al sistema y si corresponden a la realidad de un usuario autorizado propio de la institución.
Control de las nuevas aplicaciones	Revisar los permisos de *root* ante el ingreso de otros sistemas vinculados al sistema
Análisis de los accesos de los usuarios	Controlar cada ingreso en función de las actividades de los usuarios y si estos corresponden a las acciones asignadas de cada uno

Fuente: Minerva (2017, pág. 63), Diagramado por el autor

1.3.3. Principios de la seguridad de la información

Para garantizar la SI, las organizaciones deben adoptar principios básicos, que sirven de base para buscar una mayor eficacia en esta área. Los principios más básicos adoptados son: confidencialidad, integridad y disponibilidad.

Entender los objetivos de seguridad permite dentro de la implementación exponer los parámetros a seguir por parte de usuarios y colaboradores sobre la Norma ISO 27001 y como se deben dar sus labores dentro de la institución, en este sentido, la SI determina los preceptos necesarios para que se establezca la protección de la información sobre cualquier tipo de amenaza como un intento de garantizar que esta información sea entregada manteniendo intactas los tres principios mencionados. Como se muestra en la tabla 1.3, según Hoepers, y Steding-Jenssen (Hoepers & Steding-Jessen, 2014, pág. 12), estos atributos son los siguientes:

Tabla 1.3 ***Atributos de la SI***

Atributo	Descripción
Confidencialidad	Consiste en la garantía de que únicamente las personas autorizadas posean acceso a la información almacenada o transmitidas por medio de las redes de comunicación, mantener la confidencialidad presupone asegurar que las personas no tengan conocimiento de la información sensible para la empresa de forma accidental o premeditada, sin que tengan acceso autorizado para dicho procedimiento.

Integridad	Consiste en la fiabilidad de la información. Indica una conformidad de los datos almacenados con respecto a las inserciones, alteraciones y procesamientos autorizados que se efectúan, indica así mismo, la conformidad de los datos transmitidos por los emisores con los recibidos por los destinatarios. El mantenimiento de la integridad presupone la garantía de no violación de datos con la intención de alterarlos, copiarlos o borrarlos, sea de manera accidental o a propósito
Disponibilidad	Consiste en la garantía de que la información se encuentre accesible a las personas y a los procesos autorizados en cualquier momento en el que sean requeridos, durante los periodos de tiempo acordados entre los que administran la información y el área de informática. Así mismo, mantener la disponibilidad de la información implica que se garantiza la prestación continua de los servicios sin interrupciones en proporcionar información a quién sea autorizado para recibirla

Fuente: Hoepers, y Steding-Jenssen (2014, pág. 12), Diagramado por el autor.

El uso adecuado de los principios antes mencionados, puede proporcionar un entorno seguro, para que las organizaciones desarrollen su trabajo. Los principios básicos de la SI son de suma importancia para combatir las amenazas de la información que aprovechan las vulnerabilidades existentes y deben definirse para que puedan generar resultados más efectivos (Hoepers & Steding-Jessen, 2014, pág. 13).

1.4. Gestión de riesgos

Las amenazas y vulnerabilidades constituyen un tema recurrente para comprender la SI a través de medidas de gestión de riesgo, en el sentido de que se deben conocer los riesgos tecnológicos que existen para las organizaciones y, por lo tanto, tomar las medidas de seguridad necesarias. Para Turban, y Volonino, (2013) citados por Marques (2018, pág. 34), uno de los principales errores que comentan los gerentes o directores es no dar la debida importancia al tema, sin conocer las vulnerabilidades y amenazas presentes en la organización. Por lo tanto, como una forma de entender, demostrarán cuáles son las amenazas y vulnerabilidades, así como los métodos y procedimientos de seguridad y la investigación de riesgos.

1.4.1. Vulnerabilidades

Podemos entender por vulnerabilidades los fallos que tiene un sistema, lo que puede causar la falta de disponibilidad de la información, o incluso el incumplimiento de la confidencialidad y el cambio sin autorización, y puede deberse a un grupo de elementos, como la carencia de capacitación, la falta de mantenimiento, controles de acceso, falta de

protección de un área en particular amenazada (Joya & Sacristán, 2017), por ejemplo, crear cuentas en el sistema sin especificar las restricciones y permisos. Joya y Sacristán (2017), explican que las vulnerabilidades se pueden clasificar en tres tipos, como se muestra en la tabla 1.4:

Tabla 1.4. ***Características de las vulnerabilidades que pueden presentarse en sistemas de gestión de la información***

Vulnerabilidades	Características
Tecnológico	Comprende redes de computadoras, computadoras, amenazas de virus, piratas informáticos, en resumen, todas las actividades relacionadas con la tecnología
Físicos y ambientales	Representado por el entorno en el que se encuentran las computadoras y los periféricos, por ejemplo: ausencia de generador de energía, normas para contraseñas, entre otros, así como, los eventos naturales o eventos catastróficos de origen humano o natural, que impliquen la perdida de información.
Humano	Esta categoría incluye el factor humano, que se considera el más difícil de evaluar, porque incluye características psicológicas, emocionales y socioculturales que varían de persona a persona. Por ejemplo: falta de capacitación, calificación, ambiente organizacional inapropiado para el desarrollo de actividades, entre otros

Fuente: Joya y Sacristán (2017), Diagramado por el autor.

1.4.2. Amenazas

Cuando un activo de información sufre un ataque potencial, u ocurre un incidente no deseado con alguno de los activos, podemos entenderlo como una amenaza. Este ataque puede ser llevado a cabo por agentes externos (empresas, personas que no son empleados de la organización) o internos, en este sentido, las amenazas son más evidentes en las instituciones que presentan algún tipo de interconexión a la red, por esta vía (Internet), aumenta el nivel de exposición de vulnerabilidades con lo cual, se genera la posibilidad de acceder a la información institucional, incluso sin autorización si hay agujeros de seguridad (Campo, 2013, pág. 22).

Estos sistemas, que utilizan estos nuevos estándares de red, aumentan considerablemente las vulnerabilidades, ya que la comunicación también se puede realizar a través de redes de datos inalámbricas, que a su vez son difíciles de proteger debido a los diversos puntos de acceso, lo que lo hace aún más el incumplimiento de la confidencialidad de la información.

Existen varios tipos de amenazas, Sémola (2003), citada por Campo (2013, pág. 22) las clasifica en las siguientes categorías como se muestra en la tabla 1.5:

Tabla 1.5. ***Clasificación de las Amenazas***

Amenaza	Descripción
Natural	Hace relación a fenómenos naturales como por ejemplo incendios, inundaciones, terremotos, tormentas, contaminación, entre otros.
Involuntarios	Son generados sin alevosía y pueden ser causados por accidentes, errores, falta de energía, etc.
Voluntarios	Son intencionados, provocados por agentes humanos como hackers, invasores, espías, ladrones, creadores y diseminadores de malware, incendiarios, etc.

Fuente: Campo (2013, pág. 22), Diagramado por el autor.

1.4.3. Riesgos asociados a la seguridad de la información

El riesgo es "*una combinación de una amenaza que aprovecha alguna vulnerabilidad de un activo para impactarlo y causarle daño*" (Restrepo, 2018, pág. 284). Validar cuales son estos, permite conocer cuáles tienen un mayor grado de incidencia y hacia donde incrementar los esfuerzos de control informático. Los factores de riesgos de mayor incidencia son principalmente los activos y las vulnerabilidades (Restrepo, 2018, pág. 285). Un activo de información es "*algo a lo que una organización le asigna un valor y, por lo tanto, la organización debe proteger*" (Armijos, 2018, pág. 91).

Estas se clasifican en: Activos de información (datos), activos de software (aplicaciones), activos físicos (computadoras, medios magnéticos), documentos de papel (contratos), imagen de la institución y reputación (historiales empresariales), personal (usuarios y clientes), servicios (comunicados) (*Ibid.)*. Por su parte, las vulnerabilidades están determinados como "*los puntos débiles relacionados con los activos organizacionales, operacionales, físicos y de sistemas dentro de las organizaciones*" (Mier, 2017, pág. 57). "Los niveles de vulnerabilidad se pueden valorar en función de: severidad, efecto en el activo, y el grado de exposición" (Guamán, 2015).

Por su parte, las vulnerabilidades son acciones que pueden causar daño en un activo de las unidades educativas. La clasificación según la Norma ISO (2013) es "*fuerza mayor, deficiencias organizacionales, fallas humanas, fallas técnicas y actos deliberados*" (pág. 23). Según expone Armijos (2018, pág. 166), en la evaluación de los peligros se debe

tomar en cuenta la implementación de diversas etapas, a saber, la valoración del riesgo, la evaluación del riesgo, el análisis de este, y por último la gestión del mismo.

Según el recién citado autor (*Ibid.)*, la valorización consiste en "*analizar las amenazas a un sistema de información, las vulnerabilidades del mismo y el impacto potencial*" (p. 166) si se incorporan las mismas, mientras que la Evaluación, es la medición del nivel de impacto de las amenazas ante el sistema y la información. Por su parte, el Análisis de riesgo, consiste en evaluar los niveles de peligro activos sobre las amenazas y vulnerabilidades y, por último, la Gestión se corresponde con el un conjunto de estrategia efectiva en función del costo, tratamiento y procedimiento realizado.

1.5. Normativas para la gestión de seguridad y riesgos de la información

La gestión de riesgos de seguridad de la información es el proceso de identificar, evaluar y reducir los riesgos a un nivel aceptable e implementar los mecanismos correctos para mantener ese nivel de riesgo (Cárdenas, Martínez, & Becerra, 2016). Por lo tanto, la evaluación de riesgos es un componente crítico en el trascurso del periodo de tratamiento y control de los riesgos de la SI. La gestión eficaz del riesgo depende de una evaluación de riesgos sólida, también conocida como análisis de riesgos, que es un paso para el reconocimiento y valoración de los riesgos de manera precisa o las pérdidas potenciales asociadas con las vulnerabilidades de los activos de información, todo esto es esencial para el desarrollo de un proceso de control de riesgos y estrategias de protección efectivos (Wang & Ratchford, 2018).

Existen dos enfoques generales para la evaluación de riesgos: enfoque cuantitativo y enfoque cualitativo. El enfoque cuantitativo utiliza datos numéricos, fórmulas y cálculos para obtener una medida objetiva de los riesgos. Una formulación matemática típica de riesgo utiliza un nivel más bajo de desagregación de amenaza y probabilidad para determinar el valor, exposición, frecuencia y medidas de protección existentes de un activo (Ghazouani, Faris, Medromi, & Sayouti, 2014).

El enfoque cualitativo es más subjetivo y utiliza opiniones y percepciones de expertos sobre la probabilidad y el impacto de un riesgo para determinar el nivel de riesgo. Tanto los enfoques cuantitativos como los cualitativos tienen sus propias fortalezas y limitaciones. Para una evaluación de riesgo típica, se debe seleccionar un enfoque o

metodología apropiados basados en la misión comercial y las necesidades de evaluación. Además, se deben identificar los activos críticos y las vulnerabilidades y amenazas relevantes (Cárdenas, Martínez, & Becerra, 2016).

Existen diversas metodologías de investigación y evaluación de riesgos disponibles actualmente, como se muestra en la Tabla 1.6. Estas, son principalmente de naturaleza cuantitativa o cualitativa que abordan diversas dimensiones de los riesgos de SI, y una organización a menudo se enfrenta a la difícil tarea de adoptar la metodología óptima o más adecuada. El objetivo común de las metodologías de evaluación de riesgos es alcanzar la estimación del valor general del riesgo y la adecuación de la metodología debe ajustarse a las necesidades de la organización (Vorster & Labuschagne, 2005).

Tabla 1.6. ***Diversas metodologías para el análisis de la gestión de riesgos de la información***

Métodos de gestión de riesgos	**Herramientas de métodos de gestión de riesgos**
• CIS Critical Security Controls • Control Objectives for Information and Related Technology (COBIT) • CCTA Risk Assessment and Management • Dutch A&K Analysis • EBIOS • ETSI • Factor Analysis of Information Risk (FAIR) • Fundamental Information Risk Management (FIRM) • Failure Modes and Effects Analysis (FMEA) • Facilitated Risk Assessment Process (FRAP) • Information Risk Assessment Methodologies (IRAM) • ISAMM • Information Security Forum (ISF) Methods • ISO TR 13335 (a Technical Report which is a precursor to ISO/IEC 27005); • ISO/IEC 27001 • ISO/IEC 31000 • Methodology for Information Systems Risk Analysis and Management (MAGERIT) • MEHARI • MIGRA • NIST SP 800-30 • NIST SP 800-39 • NSA IAM / IEM / IA-CMM • OCTAVE • Open Web Application Security Project (OWASP) • Manual (OSSTMM) • PCI Security Standards Council • Practical Threat Analysis (PTA) • SANS 20 • Simple to Apply Risk Assessment (SARA) • Security Officers Management and Analysis • Project (SOMAP) • Simplified Process for Risk Identification (SPRINT)	• Acuity Stream • Acuity Stream • Archer • Axur • Callio • Methodology (CRAMM) • Casis • Citicus ONE • Cobra • CRAMM • EAR / PILAR • EBIOS • GSTool • GxSGSI • ISAMM • Módulo Risk Manager • Proteus Enterprise • RA2 Art of Risk • Resolver Ballot • Resolver Risk • Risicare • Riskwatch • RM Studio • Risk Manager • RiskOptix • MIGRA • RSAM • vsRisk

Fuente: Ghazouani y col. (2014).

Como se ve en la Tabla 1.6, no hay escasez de guías, enfoques metódicos e instrumentos de soporte, todas estas, apuntan a un análisis objetivo destinado a determinar la cantidad de riesgo a la que están sujetos varios activos y sistemas de TI. Según los creadores del método MAGERIT, el desafío de todos estos enfoques "*es la complejidad del problema que enfrentan, una complejidad en el sentido de que hay muchos elementos a considerar y que, si no son rigurosos, las conclusiones serán poco confiables*" (CSAE, 2012a).

Entre todas estas metodologías, las más empleados son COBIT, ITIL, La familia ISO (específicamente el estándar ISO 27005 que contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en SGSI), y la MAGERIT, a continuación, se presentan los aspectos más relevantes de las metodologías COBIT, ITIL, y de la familia ISO, la metodología MAGERIT se describe más adelante por ser la empleada en el presente estudio.

1.5.1. COBIT

COBIT es un marco de gobierno de tecnología de la información que define un conjunto de mejores prácticas para controlar la tecnología de la información dentro de las organizaciones. Fue creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA), en 1995 como un sistema estándar global hacia negocios para generar controles de los sistemas de información, alcanzando un posicionamiento en 98 países. Su segunda edición fue emitida en 1998 agregando un control de alto nivel y "un sistema adjunto vía CD-ROM con todo el contenido operativo y manuales adjuntos de servicio" (COBIT, 2019, pág. 2).

Dicho sistema permite a los administradores organizacionales controlar aspectos técnicos y de alto riesgos por medio de un modelo que emite una auditoria de gestión de los sistemas de información. Por lo expuesto, emite un beneficio directo para administradores y auditores hacia un mayor entendimiento de las características y procesos que se deben sostener en las tecnologías de la información por medio de la monitorización y desarrollo.

También reconoce a los gerentes la capacidad de cerrar la grieta entre los requisitos de control, los problemas técnicos y los riesgos comerciales. COBIT a su vez, "*enfatiza el cumplimiento normativo y ayuda a las organizaciones a aumentar el valor obtenido*" (Sanchez, 2011) del departamento de tecnología de la información dentro de las organizaciones. El punto central de adoptar COBIT es administrar la información con recursos de TI para garantizar la operación comercial adecuada de la organización.

1.5.2. ITIL

ITIL (*Information Technology Infrastructure Library)* es un conjunto de publicaciones que mejoran las prácticas para gestión de servicios a nivel de las tecnologías de información bajo un asesoramiento sobre la provisión de servicios con altos parámetros de calidad. Para esto, "*se enfoca en cinco etapas: estrategia, diseño, transición, operación y mejora continua*" (Information Technology Infrastructure Library, 2019, pág. 6).

Este proceso otorga ayuda en la institución para ejecutar las mejores prácticas en tecnologías de información, independientemente del tamaño o sector al que pertenezca la organización. Para comprender la relevancia de ITIL, es pertinente entender la relación entre la tecnología de información y el éxito que se da bajo un correcto manejo previo de la administración institucional.

1.5.3. La familia de la norma ISO/IEC 27000

La seguridad de los SI, abarca a todos los servicios de la organización: recursos humanos, marketing, ventas, finanzas, entre otros. De hecho, la seguridad requiere la participación de todos, independientemente de su nivel jerárquico (Cohard, 2019). Los estándares de la serie ISO 27000 son "*la base para establecer un sistema de SI, por su parte, el estándar 27002 también especifica que el documento del sistema de SI debe ser aprobado por la administración, publicado y distribuido a los empleados y partes interesadas externas*" (Tersek, 2008), en otras palabras, es el apoyo administrativo que le da legitimidad e importancia al sistema de gestión de seguridad de los activos informáticos (Cohard, 2019, pág. 265).

Los estándares de la serie 27000 son diversos, al punto de llegarse a conocer como familia de normas, estas, se detallan en la Tabla 1.7:

Tabla 1.7. ***Ejemplos de estándares de la serie ISO 27000***

Norma	Contenido
ISO 27000	Es la norma que proporciona una visión general de los sistemas de gestión de seguridad de la información y contiene los términos y definiciones que se utilizan en las diferentes aplicaciones de dicha norma
ISO 27001	Corresponde a la norma principal de la serie 27000 (última actualización en 2013) y que contiene los diferentes requisitos para "establecer, implementar, mantener y mejorar continuamente un SGSI en las organizaciones independiente de su tipo, tamaño o naturaleza" (ISO, 2013, pág. 9). En este apartando también se incluyen los requisitos para la valoración y el tratamiento de riesgos de SI.
ISO 27002	Se centra en las buenas prácticas para gestión de la SI
ISO 27003	Focaliza su atención en los aspectos necesarios para un diseño exitoso y una buena implementación del SGSI
ISO 27004	Se encarga de especificar la estructura del sistema de medición, cuáles son los parámetros a medir, tiempos y parámetros. Además, permite a las organizaciones el establecimiento de objetivos relacionados con el rendimiento y los criterios de éxito.
ISO 27005	Establece los lineamientos para la gestión de riesgos de SI. De esta forma, se exponen los requerimientos que se deben tomar en cuenta para el proceso de valoración de riesgos, relacionados con la identificación, análisis, evaluación y tratamiento de los mismos.
ISO 27006	Apoyar la acreditación de organismos de certificación que brindan la certificación del SGSI. Aquí se exponen los requisitos y provee una guía para la auditoría y la certificación del sistema
ISO 27007	Proporciona el marco de seguridad para desarrollar, implantar y mantener especificaciones de los Sistemas de Gestión de la SI aprovechable en cualquier tipo de organización que requiera de su incorporación
ISO 27008	Es una plataforma estratégica de implementación y operación de los controles según el tipo de empresas
ISO 27009	Permite la interpretación de los requisitos acorde a la organización donde se va instaurar
ISO 27010	Determina como va ser el traslado e intercambio de la información desde una perspectiva de funcionamiento interno

Fuente: obtenido de ISO (2013), Diagramado por el autor.

La norma ISO 27000, como se mencionó en los acápites previos, es el documento básico que proporciona una visión general de la norma y sus elementos de vocabulario. Los términos pueden tener varias definiciones de la vida cotidiana con lo cual, esta norma permite la adaptación de un vocabulario común sobre seguridad. La norma también explica los principios del SGSI (SGSI).

Esta familia de normas, son aplicables a todo tipo de empresas, es lo suficientemente flexible como para integrarse en los sistemas de gestión existentes y los diferentes enfoques de riesgo existentes dentro de la organización (ISO, 2018).

El código de buenas prácticas para la gestión de seguridad de los SI se encuentra en la ISO 27002. Este es el punto de partida para el desarrollo de guías de buenas prácticas específicas para la organización. No todos los elementos deben ser aplicados; es necesario seleccionar aquellos que son relevantes para la organización en su contexto. Este conjunto de buenas prácticas debe ser mantenido cerca por los gerentes de seguridad de SI y debe ser comunicado regularmente en un lenguaje apropiado al personal para crear conciencia. Además, la norma 27002 incluye una sección dedicada a la seguridad de los recursos humanos antes, durante y después del período de empleo. Este estándar puede desempeñar el papel de un repositorio de SI en la organización.

Por su parte, El estándar 27037 proporciona orientación a los responsables de recopilar y preservar la evidencia digital. Esta evidencia proviene de varias fuentes y generalmente de los archivos de registro de eventos, los cuales, registro generalmente incluyen una marca de tiempo, el origen y el destino de los flujos (por ejemplo, la dirección IP), el usuario en cuestión y los datos accedidos o transmitidos. El borrado de rastreo es parte del proceso utilizado por los piratas informáticos, por lo que generalmente intentan borrar estos archivos. La gestión de los derechos de archivo juega un papel importante aquí (Cohard, 2019).

En resumen, los estándares presentados en este capítulo como parte de la familia de normas ISO 27000, ayudan a estructurar la implementación de un SGSI en la organización. Este enfoque debe ser global: físico (acceso), humano, sistema y ser parte de los procesos de la organización.

La familia de normas ISO / IEC 27000, es una serie grande y creciente de normas desarrolladas, publicadas y mantenidas por un esfuerzo conjunto de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). ISO 27000: 2016 es el documento líder de la norma y describe las otras normas de la familia (ISO, 2016).

Excepto por las normas ISO 27000 específicas del sector, todas las normas ISO son universalmente aplicables (Siponen & Willison, 2009), pero es posible que sea necesario realizar un paso de operacionalización antes de aplicarlas, en parte debido a su naturaleza única.

Por ejemplo, al aplicar los 114 controles en ISO 27002:2013, la organización debe seleccionar qué controles son aplicables a la organización (ISO, 2013), y debe identificar si falta algún control.

1.5.4. Entorno del estándar ISO/IEC 27001:2013

La norma ISO 27001:2013 (ISO, 2016) es el estándar más conocido de la familia ISO 27000 y contiene los requisitos de un SGSI (ISO, s.f). Un SGSI es un instrumento de gestión de alto nivel que tiene como objetivo ayudar a las organizaciones a implementar un marco "*para gestionar la seguridad de los activos de información*" (ISO, 2016).

La ISO 27001:2013 también contiene un Anexo conocido como "A", que establece controles y objetivos de control para aumentar la SI en un nivel más operativo, estos, se derivan y se alinean directamente con los controles establecidos en ISO 27002:2013 (ISO, 2013), que proporciona una guía de implementación para estos controles. En todo el mundo, hay más de 1.6 millones de organizaciones que tienen una certificación ISO 27001 (ISO, 2017).

Esta normativa, está comprendida como un SGSI, que a su vez, es "*la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la SI*" (ISO, 2013, pág. 4). En esta normativa se define a la SI como la "*preservación de la confidencialidad, integridad, no repudio y confiabilidad*" (ISO, 2013, pág. 5).

La implementación de la norma requiere tener en cuenta las siguientes 14 dimensiones (ISO, 2013):

- El contexto de la organización;
- Liderazgo y compromiso;
- Objetivos del SI;
- La política de SI;
- Roles, responsabilidades y competencias;
- Gestión de riesgos;

- Monitoreo del desempeño e indicadores clave de desempeño;
- Documentación;
- La comunicación;
- Habilidades y conciencia;
- Relaciones con proveedores;
- Auditoría interna;
- Administración de incidentes;
- Mejora continua.

1.5.5. Generalidades para la selección de un sistema de gestión de riesgos

Los sistemas de gestión de riesgos, proporcionan un modelo y estructura para organizar y clasificar los riesgos y los controles internos asociados a estos, para así ayudar a las organizaciones a monitorear y medir la efectividad de sus actividades e inversiones.

Este objetivo generalmente se logra a través de un conjunto de metas de control descritos en cada marco operativo, el cual, como se vio anteriormente, busca facilitar a la organización evaluar las políticas de seguridad y establecer objetivos para mejorar los procedimientos para proteger los sistemas y los datos.

Como se desprende de la teoría hasta ahora citada en esta investigación, otro beneficio significativo de aprovechar un marco de cumplimiento especifico, es que puede ayudar a una organización a priorizar y coordinar actividades, que garanticen la SI.

Es importante tener en cuenta que, a lo largo de los años los profesionales de la tecnología de la información han visto un aumento en los mandatos regulatorios requeridos que deben ser respaldados, y también se les presenta un número creciente de marcos y metodologías para gestionar el riesgo de la tecnología de la información de manera verificable y medible.

La abundancia de literatura sobre el uso de metodologías como la ISO 27001, dan a entender que esta es ampliamente aceptada como una práctica estándar para que las organizaciones evalúen, supervisen y midan la efectividad de sus inversiones en seguridad y cumplimiento.

Sin embargo, como se aprecia en la Tabla 1.6, son realmente muchas las metodologías existentes que buscan el análisis de riesgos. Si bien algunos marcos, como el SANS 20, están técnicamente orientados y son explícitos en las tecnologías y los controles de seguridad a aplicar, otros se refieren más a las mejores prácticas y pautas recomendadas.

Independientemente del enfoque, el objetivo del marco es proporcionar recomendaciones y orientación para permitir que se establezcan prácticas y procedimientos para crear valor comercial y minimizar el riesgo. La Tabla 1.8 describe los marcos más comunes y sus casos de uso, estos, no depende del tipo de negocio para ser implementado.

Tabla 1.8. ***Diferentes marcos de gestión de riesgos y sus características***

Nombre	Organización	Descripción:	Controles de seguridad
Payment Card Industry Data Security Standard (PCI DSS)	PCI Security Standards Council	Inicialmente desarrollado en 2004, el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) es un estándar de SI que describe 12 requisitos de seguridad para cada organización que acepta tarjetas de crédito como Visa, MasterCard, American Express y otras. El PCI Security Standards Council es un foro global para el desarrollo continuo, la mejora, el almacenamiento, la difusión y la implementación de estándares de seguridad para la protección de datos de cuentas. Al cumplir con las regulaciones PCI, puede asegurar sistemas críticos y proteger los datos confidenciales del titular de la tarjeta.	12 Requisitos organizados en seis grupos de objetivos de control.
CIS Critical Security Controls	Center for Internet Security (CIS)	Originalmente desarrollado en 2008, los controles críticos de seguridad del Centro de seguridad de Internet para la ciber defensa efectiva (conocidos como los 20 principales controles de CIS) son un conjunto de acciones recomendadas para la ciber defensa que proporcionan formas específicas y procesables para frustrar ataques potentes.	20 controles CIS
OWASP	Open Web Application Security Project (OWASP)	El *Open Web Application Security Project* (OWASP) es una organización benéfica mundial sin fines de lucro centrada en mejorar la seguridad del software de la aplicación. Los 10 principales riesgos de seguridad de aplicaciones web de OWASP brindan orientación a los desarrolladores y	10 controles

		profesionales de seguridad que se dirigen a las vulnerabilidades más críticas que se encuentran y explotan comúnmente en las aplicaciones web. El OWASP Top 10 no es una lista exhaustiva de elementos de riesgo, pero proporciona un punto de partida sólido para las organizaciones que buscan fortalecer la postura de seguridad de su entorno de aplicaciones web.	
NIST 800 series	National Institute of Standards and Technology (NIST)	NIST SP 800-53 describe una estrategia integral combinada con varios controles de seguridad para el monitoreo continuo, diseñado para permitir una mejor toma de decisiones basada en el riesgo. Otro conjunto popular de controles NIST es 800-171. La principal diferencia entre NIST 800-53 y 800-171 es que este último se desarrolló específicamente para proteger datos confidenciales sobre contratistas y otros sistemas de información no federales.	NIST 800-53 y 800-171
ISO/IEC 27000	International Organization for Standardization (ISO)	ISO proporciona una familia de estándares para ayudar a las organizaciones a proteger los activos de información. Cada estándar está diseñado para proporcionar orientación en relación con un conjunto específico de actividades centradas en un conjunto específico de objetivos. Por ejemplo, la construcción de la base de un programa de seguridad está cubierta en ISO 27001, la implementación de controles detallados está cubierta en 27002 y la gestión de riesgos está cubierta en 27005	ISO/IEC 27001
Information Technology Infrastructure Library (ITIL)	Information Technology Infrastructure Library (ITIL)	(ITIL) es un marco de mejores prácticas para la prestación de servicios de TI. ITIL v3 se compone de cinco volúmenes distintos: *ITIL Service Strategy*; Diseño de servicios ITIL; Transición del servicio ITIL; Operación del servicio ITIL; e ITIL Mejora continua del servicio.	ITIL en sí no proporciona una guía prescriptiva sobre los controles y se basa en otros marcos como ISO para ese aspecto de la gestión de la seguridad. ITIL se centra más en las actividades más amplias y la relación con la seguridad de la prestación de servicios y el soporte.

Factor Analysis of Information Risk (FAIR)	FAIR Institute	FAIR es un marco para comprender, analizar y medir el riesgo de la información. Basic FAIR proporciona un marco compuesto por 10 pasos en 4 etapas diseñados para cuantificar y comunicar el riesgo de manera consistente en toda la organización.	
OCTAVE	Software Engineering Institute, Carnegie Mellon	OCTAVE fue desarrollado por el equipo de respuesta a emergencias informáticas de la Universidad Carnegie Mellon (más comúnmente conocido como CERT). Este marco de seguridad ofrece un enfoque estratégico para la SI.	
COBIT	Information Systems Audit and Control Association (ISACA)	COBIT es un marco de gestión y gobierno que define y organiza controles implementables que se organizan en procesos relacionados con TI.	COBIT5 Prácticas de gobierno y gestión

Fuente: Diagramado por el autor, Información recabada desde las webs de cada institución que creo el respectivo método.

Aprovechar los estándares de la industria proporciona un nivel de garantía de que la organización y los socios comerciales siguen las mejores prácticas para proteger los sistemas y los datos.

No hay un estándar único para todos los tipos de negocios cuando se trata de seleccionar un marco de seguridad. En este sentido, al iniciase un proyecto de gestión de riesgos y vulnerabilidades, es importante comprender qué políticas debe cumplir la organización; y qué marcos de gestión de riesgos ya se han implementado.

En algunos casos, los marcos normativos como la ISO 27001 pueden complementar las implementaciones de marcos ISO existentes. En otros, los mandatos verticales y de cumplimiento de la industria pueden desempeñar un papel más importante en la selección del marco. Por ejemplo, COBIT puede estar mejor alineado para cumplir con SOX. Por su parte, ISO 27000 ofrece amplitud y aplicabilidad en todas las industrias, pero es más probable que se adopte cuando una empresa necesita comercializar la certificación ISO.

De igual forma, los controles NIST SP 800-53 se diseñaron específicamente para agencias del gobierno de EE.UU., pero también proporciona estándares de SI que son aplicables en todos los niveles de varios tipos de industrias.

1.6. Establecimiento de un SGSI

Como se mencionó en los acápites anteriores para la implementación de un SGSI, es necesario considerar de manera oportuna la valoración de los activos presentes y del riesgo que estos poseen, Kopertti (2018, pág. 352), al respecto explica que el análisis del riesgo implica el empleo de los SI disponibles para así, lograr conocer las fuentes de riesgo y estimar el nivel del mismo. El objetivo de esta acción es "*identificar y calcular los riesgos basados en la caracterización de los activos, y en el cálculo de las amenazas y vulnerabilidades*" (Galarza, 2018, pág. 139).

Según indica Chamorro (2013) "*los riesgos se calculan de la combinación de los valores de los activos, que enuncian el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se agrupen*" (pág. 64) y provoquen un incidente.

El proceso del tratamiento a nivel del riesgo según la Norma ISO (2013) busca "*reducir, aceptar, transferir y evitar los mismos*" (pág. 124). El análisis y evaluación de riesgos permite que la implementación del diseño predisponga las variables que pueden afectar la ejecución del SGSI y reducir su impacto en las fases preliminares de control.

1.6.1. Activos de la información

Cualquier componente asociado con la organización, que tenga valor o negocio, y que necesariamente necesite protección, se considera un activo de información (ISOTools Excellence, 2017).

Según se desprende de la interpretación de una lectura sobre el estándar ISO (2015), los activos de información pueden entenderse como el conjunto que involucra a las personas, la tecnología y los procesos, y que son responsables de alguna etapa del ciclo de vida de la información. Marciano & Marques (2006) conceptualiza activo como cualquier elemento que forma parte del proceso de manipulación y procesamiento de la información, los medios en que se almacena, el equipo en el que se manipula, transporta y desecha.

Para avalar que la información tenga un estándar de protección adecuado, los activos deben mapearse durante la planificación de la SI, y es extremadamente importante llevar a cabo su clasificación, que determinará el grado de confidencialidad de la información contenida en ella. La clasificación de los activos está relacionada con su grado de importancia, siendo posible clasificarlos como "muy importantes", "no importantes", etc. También es muy común clasificar por el grado de secreto que puede ser "público", información que puede llegar al público sin mayores consecuencias; "Interno" - información sobre ciertos sectores o unidades; y, "confidencial": información restringida, a la que solo pueden acceder personas autorizadas (Campo, 2013). Sin embargo, los activos, independientemente de su importancia, están sujetos a vulnerabilidades que son capaces de vulnerar la SI.

1.6.2. Metodología MAGERIT para la valoración de impacto

La metodología MAGERIT fue creada y difundida por la CSAE (Consejo Superior de Administración Electrónica) de España, "*en respuesta a la percepción de que el gobierno (Español) y, en general, toda la sociedad, depende cada vez más de las tecnologías de la información para lograr sus objetivos de servicio*" (CSAE, 2012a). Se publicó por primera vez en 1997. El análisis de riesgos usando MAGERIT está siguiendo los siguientes pasos (CSAE, 2012b):

- Determinar los activos relevantes para la organización, sus interrelaciones y su valor, es decir, qué costo sería causado por su degradación.

Los activos son los recursos en el SI o respectivos a él, que son ineludibles para que el sistema de la institución funcione educadamente y logre de esta manera alcanzar los objetivos planteados por su administración. El activo básico es la información que se maneja en sus sistemas informáticos, es decir, los datos. Otros activos relevantes pueden identificarse en torno a estos datos, por ejemplo:

"*Los servicios que se pueden proporcionar a estos datos y los servicios necesarios para poder gestionarlos…; Las aplicaciones informáticas (software) que permiten el manejo de estos datos…; El equipo informático (hardware) que aloja los datos, aplicaciones y servicios...; Los medios de información, que son dispositivos de*

almacenamiento de datos…; Los equipos auxiliares que complementan los equipos informáticos…; Las redes de comunicaciones que permiten el intercambio de datos…; Las instalaciones que albergan el equipo informático y de comunicaciones..; Las personas que utilizan u operan todos los elementos anteriores." (CSAE, 2012b, pág. 5)

- Determinar las amenazas a las que están expuestos esos activos.

Las amenazas son cosas que podrían suceder a los activos y causar daños. Hay amenazas de desastres naturales (terremotos, inundaciones, etc.) y accidentes industriales (contaminación, fallas eléctricas, etc.). Hay amenazas causadas por personas, ya sea a través de errores o ataques intencionales (CSAE, 2012a).

- Determinar qué salvaguardas están disponibles y cuán efectivas son contra el riesgo

"*Las salvaguardas o contramedidas son procedimientos o mecanismos tecnológicos que reducen el riesgo. Existen amenazas que pueden eliminarse simplemente mediante un mecanismo organizativo adecuado; Otros requieren dispositivos técnicos (programas o equipos). Otros necesitan seguridad física y la política de personal*" (CSAE, 2012a).

- Estima el impacto, definido como el daño al activo que surge de la ocurrencia de la amenaza.

El impacto es la medida del daño a un activo que surge de la aparición de una amenaza. Al conocer el "*valor de los activos y el daño causado por las amenazas, se puede derivar su impacto en el sistema*" (CSAE, 2012a).

- Apreciar el peligro, definiéndolo como el efecto ponderado en la tasa de ocurrencia (o la expectativa de aparición) de la amenaza.

El riesgo es la medida del daño probable al sistema. Al conocer el impacto de las amenazas a los activos, el riesgo puede derivarse teniendo en "*cuenta la frecuencia de ocurrencia. El riesgo aumenta con el impacto y con la frecuencia*" (CSAE, 2012a).

El objetivo declarado de MAGERIT es triple: *"(1) informar a las partes interesadas de SI sobre la existencia de riesgos y la necesidad de tratamiento, (2) ofrecer un método sistemático para analizar estos riesgos y (3) ayudar a describir y planificar las medidas apropiadas para mantener Los riesgos bajo control*" (CSAE, 2012b). Además, su objetivo es preparar a la organización para el proceso de evaluación, auditoría, certificación o acreditación, así como para promover "*la uniformidad en los informes que contienen hallazgos y conclusiones de análisis de riesgos y actividades de gestión de riesgos*" (CSAE, 2012b).

En la Figura 1.2 se muestran los elementos de análisis de riesgo potencial considerados en esta metodología. Este enfoque es consistente tanto con el modelo conceptual ISO 13335 (Sección 4.2.3).

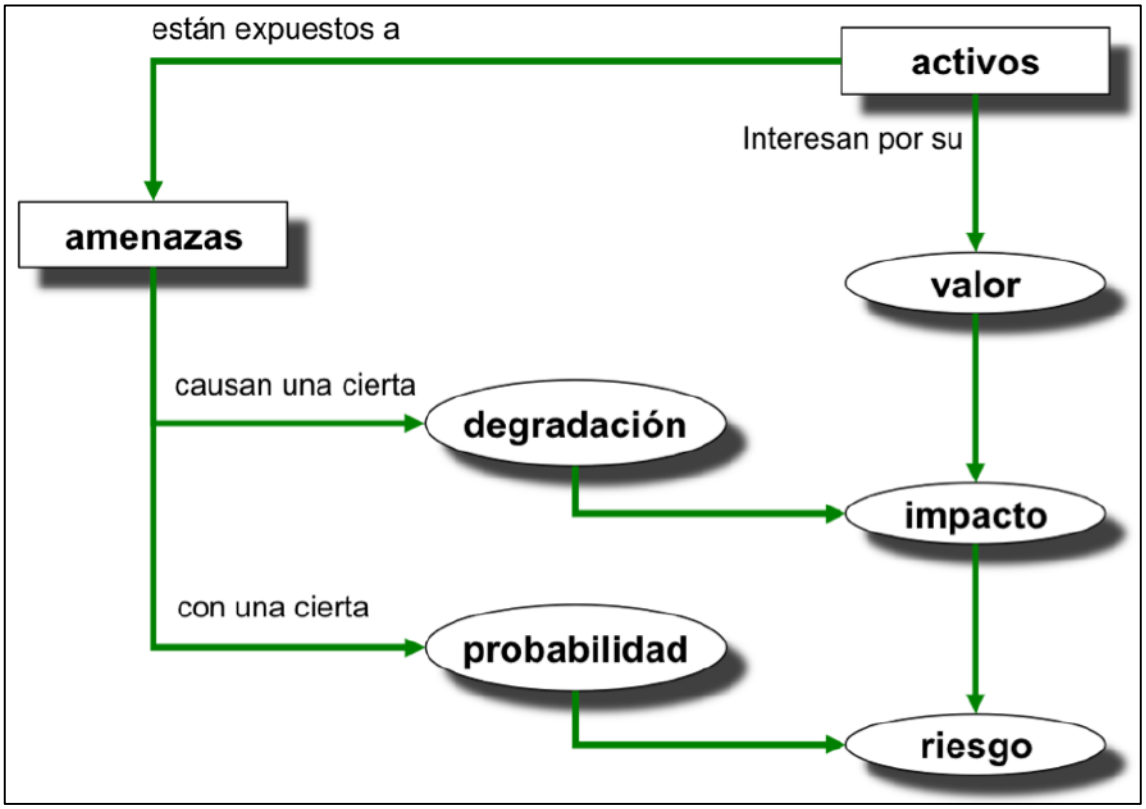


Figura 1.2. Elementos del análisis de riesgos potenciales. Disponible en: CSAE (2012a, pág. 22).

El método MAGERIT se divide en tres libros. El primero (CSAE, 2012a) describe los métodos de análisis de riesgo en detalle. El segundo, titulado "Catálogo de elementos" sirve como una especie de repositorio de "*tipos de activos, dimensiones y criterios para evaluarlos, amenazas típicas y protecciones de mejores prácticas, así como plantillas*"

(CSAE, 2012b). Finalmente, el tercer libro, "Técnicas" brinda "*información adicional y guías sobre algunas técnicas (formales) que se emplean a menudo para llevar a cabo análisis de riesgos y proyectos de gestión*" (CSAE, 2012c).

La documentación de la metodología MAGERIT, también describe cómo llevar a cabo una fase de planificación en preparación para la evaluación, así como consejos sobre cómo utilizar e integrar los resultados en una estrategia continua de gestión de riesgos. Estos, detallan la metodología de evaluación de riesgos desde tres perspectivas, cada una de las cuales implica un cierto nivel de detalle y abstracción. Primero (en el Libro 1, Capítulo 2), el método se describe a un alto nivel, adecuado para la administración y para comprender cómo la Evaluación de Riesgos debe integrarse de manera consistente con una estrategia de Gestión de Riesgos. Posteriormente, el proceso se describe a nivel operacional, especificando exactamente qué actividades se deben realizar para cada fase, así como describiendo los productos y las entradas requeridas. Finalmente, el capítulo 1 del libro 1 describe aspectos prácticos que surgen de la experiencia, mientras que el segundo y tercer libros se centran casi exclusivamente en detalles técnicos, repositorios y técnicas que pueden ser utilizados por el equipo de análisis en el momento.

CAPÍTULO 2. MARCO METODOLÓGICO

Para cumplir de manera efectiva con los objetivos que se plantean en la presente investigación es necesario definir adecuadamente los elementos metodológicos en los cuales se contextualiza el presente trabajo, estos, se describen de manera clara en los acápites siguientes.

2.1. Tipo de investigación

Esta investigación es de tipo descriptiva con implementación práctica. La descripción mencionada, está relacionada con la indagación necesaria para conocer los activos, vulnerabilidades y peligros coligados con los activos de la información con los que cuenta la institución.

Esta información es necesaria para lograr conocer la situación actual de la unidad educativa en términos de saber que elementos de un SGSI basado en la normativa ISO 27001, posee implementados la Unidad Educativa, o cuales son los aspectos que necesariamente se requieren corregir. De esta manera esta información descriptiva se convierte en los elementos de trabajo necesarios para poder generar una propuesta de SGSI adaptada a las necesidades y características de la institución.

2.2. Métodos y enfoque de la investigación

Esta investigación es de tipo cualitativa, según Sampieri y col. (2014), este tipo de investigación se caracteriza por no ser experimental y por no presentar elementos que permitan la validación de un sistema de hipótesis. En este caso, y coincidiendo con lo indicado por los metodólogos anteriormente citados, el trabajo no posee una hipótesis que requiera ser comprobada debido a que se parte de una realidad fehaciente, representados

por la inexistencia en la unidad educativa de un sistema de gestión de la información, con lo cual, se asocian una serie de riesgos y vulnerabilidades potenciales como los que se describen en el apartado teórico.

Con lo cual, se tiene además que no se generan datos estadísticos, ni mucho menos se realizan modificaciones de las variables para evidenciar un resultado, por lo que de esta manera se sustenta la afirmación de que el trabajo es del tipo cualitativo, es decir, se describe y analiza una situación y en base a esta se emite una opinión, que en nuestro caso está representada por la propuesta, que además depende de la implementación por parte del plantel para poder evaluarse un posible resultado, situación que no es parte del objeto de este estudio.

2.3. Alcance de la investigación

La investigación, posee un alcance focal, es decir, se centra en la visualización y verificación de las capacidades informáticas y el tipo de activo que maneja la Unidad Educativa Adventista Gedeón. Así mismo, solo abarcara la realización de la evaluación antes mencionada y la generación de una propuesta de implementación viable basada en las concernientes observaciones.

No es parte del alcance del presente trabajo realizar la implementación de la propuesta que se genera, porque dicha implementación. Trasciende de la decisión de la Unidad educativa como tal, y recae en la RED adventista a la cual, dicha unidad educativa está adscrita, esta es quien al final, además de aprobar la implementación y la integración con su sistema global de gestión de la información, facilitara los insumos requeridos para que la misma se concrete.

2.4. Población de estudio

Desde una perspectiva metodológica, la población de estudio está conformada por parte del universo muestral (Sampieri, Fernández, & Baptista, 2014), no obstante, en este tipo de investigación no se trabaja con una población especifica debido a que el objeto, y tipología misma del trabajo, se requiere que se consideren como parte de los individuos

relacionados con el objeto de estudio, a toda la población de la institución que de alguna manera tenga incidencia en la integridad de los activos de información, en otras palabras, se considera como parte de la población estudiada a todos el personal de la institución, así como, a todos los alumnos, representantes y público en general, no porque estos de manera particular sean evaluados sino, porque potencialmente son responsables, desde distintas perspectivas, de la integridad de la información que maneja la institución.

2.5. Técnicas e instrumentos para la recolección de datos

La técnica de recolección de datos empleada es la de la ficha de observación, estas fueron preparadas en formato Excel en base a los requerimientos de valoración de activos, riesgos y vulnerabilidades que se requieren para conocer para la generación adecuada de un SGSI.

La verificación de los activos de la información con los que dispone la institución se realizaron en una ficha con una organización como la mostrada en la Figura 2.1, mientras que las indicaciones de los elementos, y las definiciones o significados de las abreviaturas empleadas en la generación del inventario son los mostrados en la Tabla 2.1, la misma solo recoge información de los computadores ya que no existen otro tipo de activos informáticos en la institución (ver formato de tabla de inventario en los anexos).

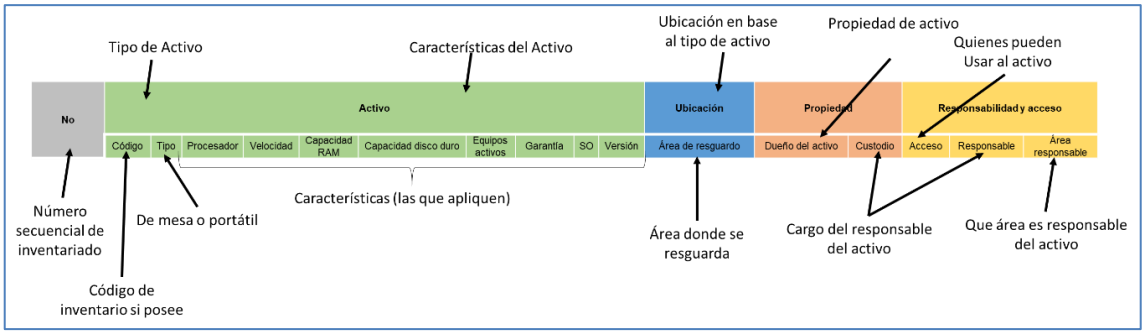


Figura 2.1. Esquema explicativo de la ficha de inventario de los activos informáticos. Diagramado por el Autor.

Tabla 2.1. ***Descripción de los elementos a emplear en la tabla de inventarios***

Elemento del Inventario	**Explicación**	**Codificación a usar**
No	Es un numero secuencial que comienza por en uno (01), solo se emplea para numerar el ítem dentro del inventario	01, 02, 03, etc.
Código	Es el código, que puede ser alfanumérico, y que está asignado al equipo (si fuera el caso), en algún inventario previo o como parte de algún proceso de control de activos	• Si aplica: Código del equipo • Si No aplica: NA (No posee código asignado en inventario previo)
Tipo	Se refiere al tipo de computador	• PC Escritorio: PCE • Laptop: Cport.
Procesador	Marca y modelo del procesador del dispositivo	Marca y modelo según sea el caso
Velocidad	Velocidad del Procesador	En Curso Velocidad del Procesador según sea el caso
Capacidad RAM	Memoria RAM que ocupa el dispositivo	Memoria RAM que ocupa el dispositivo según sea el caso
Capacidad Disco Duro	Capacidad del Disco Duro	Capacidad del Disco Duro según sea el caso
Equipos ACTIVOS	Hace referencia a que si el dispositivo se encuentra funcional	Respuesta para este ítem: SI o NO
GARANTIA	Hace referencia a si el equipo se encuentra con garantía activa del fabricante o no	• Con garantía: [En Curso] • Sin garantía: [Concluida]
SO	Se refiere al Sistema operativo y la Versión del mismo	• Windows Seven: WIN-SEVEN • Windows Vista: WIN-VIST • Windows XP: WIN-XP • Windows Server: WIN-SERV • Windows 10: WIN-TEN • Linux Ubuntu: Lix-Ubu
Versión	La versión que en este apartado debe ser documentada es la del software ofimático que emplea el dispositivo	Nombre y versión del Software ofimático según sea el caso
Área de Resguardo	Hace referencia a la dependencia donde se encuentra el dispositivo	• Dirección General: DIRG • Sub dirección: SDIR • Área Administrativa: ADM • Sala de Computación: SCOMP
Dueño del Activo	A quien pertenece el activo	• Unidad Educativa: UED • Red Adventista: RADV
Custodio	Cargo del que resguarda el equipo	• Rector: REC • Sub Director: SDIR • Director Académico: DIRAC • Personal Administración: PADM • Docente: DOCENT
Acceso	Hace referencia al personal que tiene acceso autorizado al uso del dispositivo	• Rector: REC • Sub Director: SDIR • Director Académico: DIRAC • Personal Administración: PADM • Docente: DOCENT • Estudiante: STD
Responsable	Responsable de los activos de información en el equipo	• Rector: REC • Sub Director: SDIR • Director Académico: DIRAC

		• Personal Administración: PADM • Docente: DOCENT
Área Resguardo	Área de resguardo del equipo	• Rectoría: RECT • Sub Dirección: SDIR • Dirección Académica: DIRACD • Administración: A-ADMI • Sala de computación: SCOMP

Fuente: Tabla diagramada por el Autor.

Por su parte, las vulnerabilidades, amenazas y nivel de riesgo dentro de la institución, se verificaron en un instrumento como el que se representa en la figura 2.2, y en la ***Tabla 2.2***, se muestra la interpretación de los elementos que conforman la mencionada tabla (ver formato de tabla de evaluación de vulnerabilidades y amenazas en los anexos).

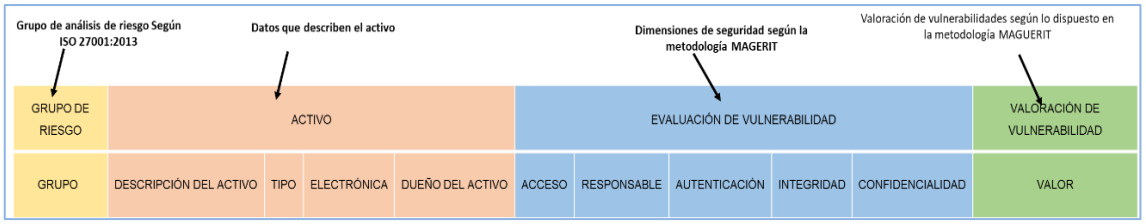


Figura 2.2. Esquema explicativo de la ficha de inventario de los activos informáticos. Diagramado por el Autor.

Tabla 2.2. ***Codificación y definición de términos en la valoración de vulnerabilidades dentro de la unidad educativa Adventista Gedeón***

Elemento del Inventario	Explicación	Codificación a usar
Grupo de riesgo	Hace referencia al aspecto operático y funcional que en base a la metodología MAGERIT e ISO 27001:2013 se evalúa	• Instalaciones • Hardware • Aplicaciones/ software • Datos/información • Redes /comunicaciones • Personal
Descripción del activo	Breve descripción del actico	Según corresponda
Tipo	Indicar si el activo es físico o digital	• Tangible • Intangible
Electrónica	Indicar que tipo de activo electrónico es, si no se trata de un dispositivo, simplemente este campo no aplica	Indicar el tipo de activo electrónico, por ejemplo: computadora, router, impresora etc.

Dueño del activo	Indicar a quien pertenece el activo	Por ejemplo: Unidad Educativa, empresa de telecomunicaciones, personal, etc.
Acceso	Indicar quien o quienes pueden ose encuentran autorizados para hacer uso del activo	• Empleados en general • Público en General • Rector, • Personal administrativo • Docentes • Representantes
Responsable	Indicar el cargo o dependencia responsable de la integridad del activo	Indicar s según sea el caso el cargo o la dependencia encargada de la integridad del activo
Autenticación	Hace referencia al nivel de importancia de la autenticación para poder usar el activo, la clasificación está basado en lo expuesto dentro de los textos de MAGERIT	• Critica • Alta • Media, • Normal • Baja
Integridad	Hace referencia a la importancia del activo, esta clasificación está basada en lo expuesto dentro de los textos de MAGERIT	• Critica • Alta • Media, • Normal • Baja
Confidencialidad	Indica el nivel de restricción para el empleo del activo. Esta clasificación está basada en lo expuesto dentro de los textos de MAGERIT	• Restringida • Protegida • Libre • Confidencial
Valor	Indica la valoración de la vulnerabilidad de los activos basada en lo expuesto dentro de los textos de MAGERIT (ver anexos 1, 2 y 3 y los libros 1 al 3 de MAGERIT	• Alta • Media, • Normal • Baja

Fuente: Tabla diagramada por el Autor.

2.6. Factibilidad técnica

En base a lo previamente indicado, en principio la evaluación de las condiciones de activos, riesgos y vulnerabilidades, es técnicamente viable debido a que existen elementos informativos que pueden ser recabados por medio de las fichas de observación antes descritas, y el evaluador (el autor de la presente investigación), posee la pericia mínima necesaria para recoger este tipo de información en los instrumentos respectivos. La factibilidad técnica de implementación reala de un SGSI se sustenta en base a los resultados obtenidos y se presenta en las secciones correspondientes.

2.7. Factibilidad operacional

La factibilidad operacional de este estudio es positiva, se cuenta para esto con la autorización de la directiva de la institución y se otorgaron los permisos y facilidades necesaria para la realización de los inventarios y las observaciones pertinente. En cuanto

a la aplicación futura, la factibilidad operacional está supeditada a la decisión de la institución en implementar en un corto, mediano o largo plazo la propuesta que se presenta, en términos generalas la implementación de la propuesta siempre será efectiva en el caso de que lo que deciden dentro de la unidad educativa aprueben la puesta en marcha de la propuesta presentada.

2.8. Modelo o estándar a aplicar

Para la presente investigación se ha seleccionado el método de evaluación de riesgos MAGERIT y los resultados de este serán adaptados aun SGSI basado en la norma ISO 27001, esto, debido a que es un método suficientemente documentado en la literatura científica y el Sistema de Gestión, en base al estándar ISO 27001, asegurara la correcta administración de los activos de información de la institución.

CAPÍTULO 3. PROPUESTA

En esta sección, se muestran los resultados obtenidos de la valoración en la institución sobre el tipo de activo de la información, así como de los riesgos amenazas y vulnerabilidades actuales. Estos resultados constituyen el soporte principal en la definición de las medidas correctivas y controles a adoptar, en otras palabras, son la base de partida para la implementación de un SGSI adaptado a la realidad y necesidades del centro educativo.

3.1. Inventario de equipos

En primer lugar, se muestra el resumen de los resultados obtenidos en el inventariado de los activos tecnológicos disponibles en la institución, estas se detallan en Tabla 3. (el detalle del inventario se encuentra en el anexo 8), como se mencionó previamente, en la Tabla 2.1, se muestran la descripción y significados de las abreviaturas que se incluyen en la siguiente tabla:

Tabla 3.1. ***Resumen por tipo del inventario de equipos tecnológicos de la Unidad Educativa Adventista Gedeón***

No	Tipo	SO	Área de Resguardo	Dueño del Activo	Custodio	Acceso	Responsable	Área Resguardo
01	PCE	**WIN-SEVEN**	ADM	UED	PADM	PADM	PADM	A-ADMI
02	PCE	**WIN-SEVEN**	ADM	UED	PADM	PADM	PADM	A-ADMI
03	PCE	**WIN-SEVEN**	ADM	UED	PADM	PADM	PADM	A-ADMI
04	PCE	**WIN10**	SDIR	RADV	SDIR	SDIR	SDIR	SDIR
05	PCE	**WIN10**	DIRG	RADV	REC	REC	REC	RECT
06	PCE	**WIN-SEVEN**	ADM	UED	PADM	PADM	PADM	A-ADMI
07	Laptop	**WIN-SEVEN**	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
08	Laptop	**WIN-SEVEN**	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
09	Laptop	**WIN-SEVEN**	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
10	Laptop	**WIN-SEVEN**	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
11	Laptop	**WIN-SEVEN**	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
12	PCE	**WIN-SEVEN**	ADM	UED	DIRAC	DIRAC	DIRAC	DIRACD
13	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
14	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
15	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
16	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
17	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP

18	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
19	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
20	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
21	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
22	PCE	**WIN-SEVEN**	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP

Fuente: Tabla diagramada por el Autor.

Inicialmente, en el inventario se puede observar que la Unidad Educativa objeto de estudio no posee una gran variedad de equipos computacionales, y a pesar de eso, dentro de su inventario, se encuentran tres computadoras que no están operativas.

Las computadoras que se listan en la Tabla 3. se encuentran distribuidas entre el área de administración, la rectoría de la institución y la sala de computación, adicionalmente, las laptops, son de uso del profesorado para las labores de docencia, así que estas se encuentran a disposición de estos cuando así lo requieran en sus actividades educativas.

Por otra parte, a pesar de que esta es una institución adventista, y que este grupo posee una interconexión operativa con una institución adventista más amplia, no se observó la existencia de ninguna red computacional institucional global, incluso, se pudo verificar por medio de una inspección ocular, que la interconexión a internet es realizada por medios del rúter provisto por la compañía telefónica que presta el servicio de internet.

Es destacable que no existe un departamento de informática en la institución, o al menos de una persona encargada del control de los equipos y sistemas, por lo tanto, también existe un desconocimiento absoluto de las normas procesos y estándares que garantizan la integridad de los activos de la información que dependan de estos elementos, así mismo, los equipos en si mayoría se encuentran desactualizados y sin un software minino de resguardo contra amenazas. Todos estos aspectos, deben ser tomados en cuanta en la propuesta de implementación del SGSI que se genere.

3.2. Identificación preliminar del nivel de vulnerabilidades, amenazas y nivel de riesgo.

En la tabla 3.2, se presenta un resumen de los activos de la información disponible, así como la respectiva clasificación de vulnerabilidad, así mismo, en la en la Tabla 2.2 se indicaron previamente las descripciones y significados de las abreviaturas empleadas a continuación (ver anexo 9 para acceder al detalle completo de esta valoración).

Tabla 3.2. ***Resumen de activos y nivel de vulnerabilidad detectados en la Unidad Educativa Adventista Gedeón***

	Descripción del activo	Tipo	Integridad	Confidencialidad	Valor
INSTALACIONES	Oficina del área administrativa	TANGIBLE	Crítica	Restringida	**Alta**
	Oficina Rectorado	TANGIBLE	Crítica	Restringida	**Alta**
	Oficina Vice Rectorado	TANGIBLE	Crítica	Restringida	**Alta**
	Oficina del Inspector académico	TANGIBLE	Crítica	Restringida	**Alta**
	Aula de computación	TANGIBLE	Crítica	Restringida	**Alta**
	Salones de clases	TANGIBLE	Crítica	Restringida	**Normal(Medio)**
HARDWARE	Computadores de mesa o laptops de uso institucional	TANGIBLE	Alta	Restringida	**Alta**
	Rúter principal de la Unidad Educativa	TANGIBLE	Alta	Protegida	**Normal(Medio)**
	Rúter principal del área de Administración	TANGIBLE	Alta	Protegida	**Normal(Medio)**
	PA Inalámbricos Wifi	TANGIBLE	Baja	Restringida	**Normal(Medio)**
	Impresoras	TANGIBLE	Baja	Libre	**Baja**
	Video Beans	TANGIBLE	Baja	Libre	**Baja**
	Teléfonos celulares personales e institucionales	TANGIBLE	Baja	Restringida	**Normal(Medio)**
APLICACIONES / SOFTWARE	Sistemas Operativos	INTANGIBLE	Crítica	Confidencial	**Alta**
	Ofimática	INTANGIBLE	Alta	Restringida	**Alta**
DATOS / INFORMACIÓN	Facturas	INTANGIBLE	Normal	Restringida	**Alta**
	Pagos del personal	INTANGIBLE	Alta	Protegida	**Alta**
	Contratos de empleados	INTANGIBLE	Alta	Restringida	**Normal(Medio)**
	Notas Académico	INTANGIBLE	Alta	Confidencial	**Alta**
	Informes psicológicos y administrativos en general	TANGIBLE	Crítica	Protegida	**Alta**

	Registros de inscripciones	TANGIBLE	Alta	Restringida	**Alta**
REDES / COMUNICACIONES	Internet	INTANGIBLE	Alta	Restringida	**Alta**
	Red de Área Local	INTANGIBLE	Normal	Restringida	**Normal(Medio)**
	Conexión Wifi	INTANGIBLE	Baja	Libre	**Baja**
PERSONAL	Administrativo	TANGIBLE	Crítica	Protegida	**Alta**
	Docente	TANGIBLE	Alta	Protegida	**Alta**
	Visitantes	TANGIBLE	Baja	Restringida	**Normal(Medio)**
	Estudiantes	TANGIBLE	Alta	Protegida	**Alta**

Fuente: Tabla diagramada por el Autor.

La metodología para la asignación de los valores de los resultados de la tabla anterior, se encuentran descritos en extenso en el libro 2 de la metodología MAGERIT (CSAE, 2012b).

Los mismos se basan en una apreciación subjetiva del evaluador en cuanto a las consecuencias para la institución por la falta, o alteración de un tipo particular de activo con respecto a las dimensiones de valoración: Integridad y Confidencialidad, dependiente ambas, por ser activos computacionales, del nivel de la seguridad para el acceso a dicho archivo (Autenticación). Según el libro 2 de MAGERIT, "*la Integridad de los datos es la propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada*" (CSAE, 2012b, pág. 15), y según ese mismo documento orientativo la evaluación de esta dimensión se realiza en base a la siguiente consideración:

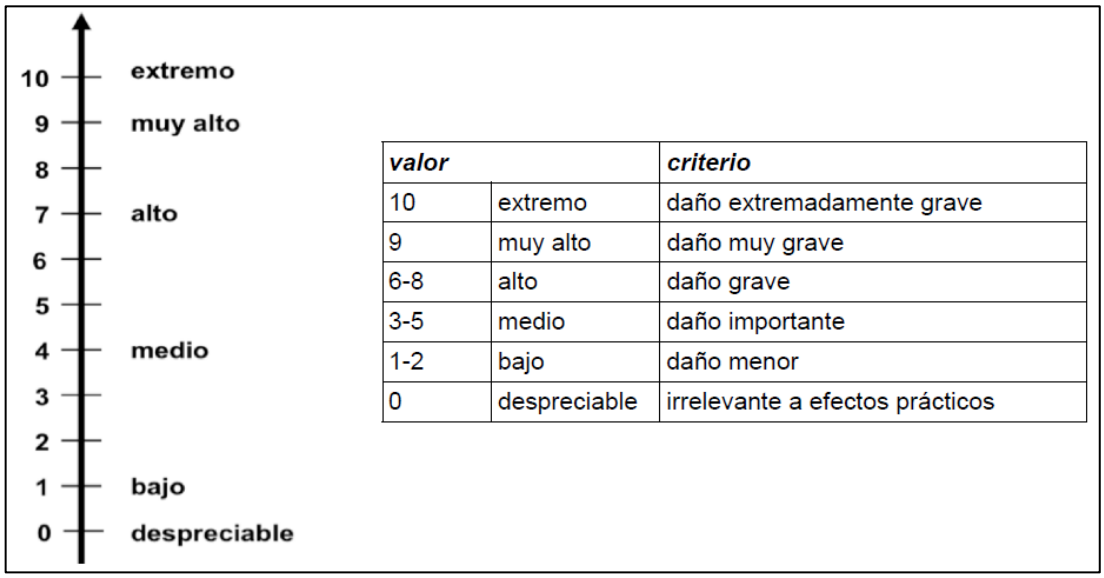
> ¿Qué importancia tendría que los datos fueran modificados fuera de control?
> Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.
> Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna. (CSAE, 2012b, pág. 15).

De la misma forma, la confidencialidad la definen como: "*Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a*

individuos, entidades o procesos no autorizados." (*Ibid*), y se evalúa en torno a la consideración interpretativa siguiente:

> "*¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?*
> *Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.*
> *Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna*." (CSAE, 2012b, págs. 15-16)

En base a lo anterior, es decir, partiendo del criterio apreciativos basado en la observación directa del elemento evaluado por parte de la persona encargada del análisis de riesgos y vulnerabilidades, y luego de la asignación de un valor "apreciativo" (Alto, medio, bajo crítico, etc.), se procede a la puntuación definitiva sustentada en lo indicado también en el libro 2 de MAGERIT (CSAE, 2012b) (Figura 3.1).



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Figura 3.1. **Criterios de valoración de riesgos y vulnerabilidades propuesto por MAGERIT. Recuperado de CSAE (2012b, pág. 19)**

Así, como se aprecia en la tabla 3.2, en la mayoría de los activos observados, se aprecia una alta proporción de casos con un nivel de vulnerabilidad elevado, por lo que si no se asumen correctivos inmediatamente los activos de la Información de la institución pueden ser vulnerados de manera intencional o no, con lo que podrá generarse perdida de información valiosa. Por su parte, como se observa en la tabla 3.3 y en la Figura 2.2, en

la inspección visual de las instalaciones de la institución se observaron una cantidad importante de amenazas y vulnerabilidades que comprometen de manera racional y latente a los activos de la información con los que cuenta la unidad educativa.

Estas detecciones, particularmente se agrupan en casi todas las amenazas posibles, por lo cual se logra entrever que es evidente la falta de implementación de un SGSI y muestran que, en la mitad de los casos, los niveles de riesgos observados estuvieron comprendidos en el rango Alto a Critico (ver detalle de esta evaluación en el anexo 12). La existencia de estos resultados, influye en el hecho de que actualmente se encuentren comprometidos dichos activos, en este caso, la inexistencia de dicho sistema, sumado con la carencia de personal dedicado al área de la gestión de la información, así como, el desconocimiento por parte de todos los actores de los riesgos y amenazas que pueden generar en este tema, son los evidentes responsables de la situación observada.

Tabla 3.3. ***Amenazas detectadas y su influencia sobre los activos de la Unidad Educativa Adventista Gedeón***

ACTIVO	AMENAZA		VULNERABILIDADES
DATOS / INFORMACIÓN	Empleo inadecuado de los datos recogidos en cualquier etapa del trabajo normal de los empleados	Datos inadecuados y manejo inapropiado de la misma	Carencias en los controles para la manipulación de la información
	Desvió de información o restricciones de salto de canales administrativos para mantener el flujo adecuado de la información	Perdida o filtración de información sensible	No existe un control de permisos y rutas administrativas adecuadas para el manejo de la información
	Acceso físico a los centros de manejo de información sin control adecuado	Acceso sin autorización ni control a las oficinas	Cualquier persona, principalmente mal intencionadas podría acceder a los dispositivos de almacenamiento de la información
	Acceso lógico con posibilidad de modificación de la información.	Acceso lógico	Modificación de la información almacenada o transmitida
SOFTWARE	Equipos dañados, por mal funcionamiento de los softwares .	Equipos disfuncionales	Los estudiantes emplean las computadoras y navegan en ocasiones sin control de los docentes en el área de computación
	Interrupción de servicios.	Interrupción de servicios	Inhabilitación del uso de las computadoras
	Errores de enraizamiento, o enrutamiento inadecuado de archivos informáticos.	Acceso a los archivos	Los archivos no son manejados bajo estándares adecuados de confidencialidad o almacenamiento.
	Acceso físico a datos informáticos sin autorización pertinente	Acceso a las computadoras sin restricciones	Perdida o hurto de información de las laptops usadas por los profesores por carencia de controles de accesos o de elementos de protección informáticos como antivirus y firewalls
	Acceso lógico con modificación de información en tránsito.	Acceso lógico a la información en transito	Los estudiantes en las sesiones de prácticas de computación utilizan las computadoras sin control ni restricciones lo que puede generar más vulnerabilidades y amenazas

HARDWARE	Accidente físico de origen varios.	incendios, terremotos	Debido a estos factores que siempre son latentes en la ciudad puede generarse la perdida de activos de la información
	Interrupción de servicios o de suministros eléctricos y de telecomunicaciones .	Interrupción de servicios	Cableado expuestos, susceptibles a robo o daño
	Acceso físico con inutilización de equipos.	Uso inadecuado de los activos	Uso inadecuado y fuera de contexto de los equipos informáticos por parte de los estudiantes
COMUNICACIONES	Accidente físico de origen varios.	incendios, terremotos	Debido a estos factores que siempre son latentes en la ciudad puede generarse la perdida de activos de la información
	Acceso físico con inutilización de equipos.	Daño de los equipos	Uso inadecuado y fuera de contexto de los equipos informáticos por parte de los estudiantes
	Interrupción de servicios o de suministros eléctricos y de telecomunicaciones .	Interrupción de servicios	Cableado expuestos, susceptibles a robo o daño
	Acceso físico con inutilización de equipos.	Acceso a los dispositivos de red	Configuración desautorizada de nuevos equipos, o des configuración o reconfiguración de los existentes
	Acceso lógico con intercepción pasiva simple de la información.	Acceso lógico de forma pasiva	Sin controles de acceso lógico configurados.
	Acceso lógico con modificación de información en tránsito.	Acceso con modificación	No se puede controlar el acceso no autorizado a la red
INSTALACIONES	Accidente físico de origen varios.	Incendios, Terremotos	Debido a estos factores que siempre son latentes en la ciudad puede generarse la perdida de activos de la información
	Interrupción de servicios o de suministros eléctricos y de telecomunicaciones .	Interrupción de servicios	Cableado expuestos, susceptibles a robo o daño
PERSONAL	Accidente físico de origen varios.	Incendios, Terremotos	Mal estado de conexiones eléctricas puede poner en riesgo los empleados y alumnos
	Mal manejo de la información	Hurto y modificación de información	Carencia de controles adecuados
SISTEMAS DE SE Y CONTROL DE ACCESO	Accidente físico de origen varios.	Incendios, Terremotos	Mal estado de varias partes de la institución
	Robos	Perdida de equipos e información	Controles insuficientes de seguridad que pueden facilitar el robo en las instalaciones
	Acceso físico con inutilización de activos.	Acceso desautorizado a las diversas áreas de la institución	Al salir de la institución el personal desconecta

Fuente: Tabla diagramada por el Autor.

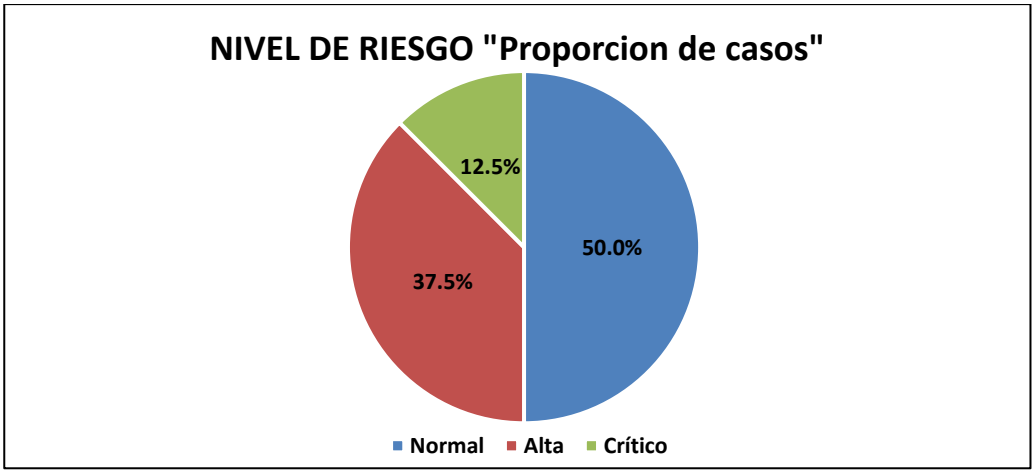


Figura 3.2. Niveles de riesgo detectados de manera general en las diversas dimensiones de evaluación

3.3. Viabilidad de la implementación

Como se mencionó en los acápites previos, la factibilidad de implementación de un SGSI en la Unidad Educativa, pasa de limitarse a la existencia ya demostrada de la necesidad de la aplicación de esta, en el caso de estudio ya los activos, amenazas y vulnerabilidades han sido detectados y se justifica en base a esto la necesidad de implementación.

No obstante la factibilidad real de implementación queda en manos de la institución, quienes después de observar la situación de esta en la materia estudiada, y la propuesta presentada en esta investigación, deberán sesionar a nivel directivo para acordar el presupuesto y las acciones administrativas que deberían implementarse para comenzar con el proceso de implementación, es decir, la necesidad existe, así como una posibilidad de enmendar la situación, pero depende de ellos que se concrete la implementación.

3.4. Cumplimiento de los requisitos indicados como obligatorios en la norma ISO 27001:2013

La evaluación de las condiciones iniciales de la institución en cuanto el cumplimiento de estándares y normativas de seguridad, también incluye la verificación de que aspectos indicados como obligatorios en la normativa ISO 27001:2013, esta valoración también es necesaria y vital ya que precisamente esta es la que indica las

carencias que deben solventarse para conseguir la adecuada implementación de la mencionada normativa. En este sentido, se verifico los puntos indicados en los apartados 4 al 10 de la norma ISO empleada (27001:2013), misma que valora aspectos como: Contexto de la organización, Liderazgo, Planificación, Soporte, Operación, Evaluación del desempeño y Mejoras. En total, son 26 ítems repartidos en los seis apartados en los que se realizó la verificación como se muestra en la Tabla 3..

Tabla 3.4*. **Requisitos de la Norma ISO 27001:2013.***

Requisito		Aspecto a considerar
4.1	Contexto de la Organización	Comprender a la organización y de su contexto
4.2		Comprender las necesidades y expectativas de las partes interesadas
4.3		Determinación del alcance del sistema de gestión de la SI
4.4		SGSI
5.1	Liderazgo	Liderazgo y Compromiso
5.2		Política
5.3		Roles, Responsabilidades y Autoridades organizacionales
6.1.1	Planificación	Acciones para tratar los riesgos y oportunidades (Generalidades)
6.1.2		Valoración de riesgos de la SI
6.1.3		Tratamiento de los riesgos de la SI
6.2		Objetivos de la SI y planes para lograrlo
7.1	Soporte	Recursos
7.2		Competencia
7.3		Concientización
7.4		Comunicación
7.5.1		Información Documentada (Generalidades)
7.5.2		Información Documentada (Creación y Actualización)
7.5.3		Información Documentada (Control de la información documentada)
8.1	Operación	Planificación y Control Operacional
8.2		Evaluación de Riesgos de SI
8.3		Tratamiento de los Riegos de SI
9.1	Evaluación del Desempeño	Monitoreo, Medición, Análisis y Evaluación
9.2		Auditoría Interna
9.3		Revisión por la Dirección
10.1	Mejora	No Conformidades y Acciones Correctivas
10.2		Mejora Continua

Fuente: Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Como se muestra en la Figura 3.3, únicamente se cumple en un 13.90% los requisitos recomendados en los apartados 4 al 10 de la normativa ISO 27001:2013. El detalle de esta evaluación se encuentra en el anexo 10.

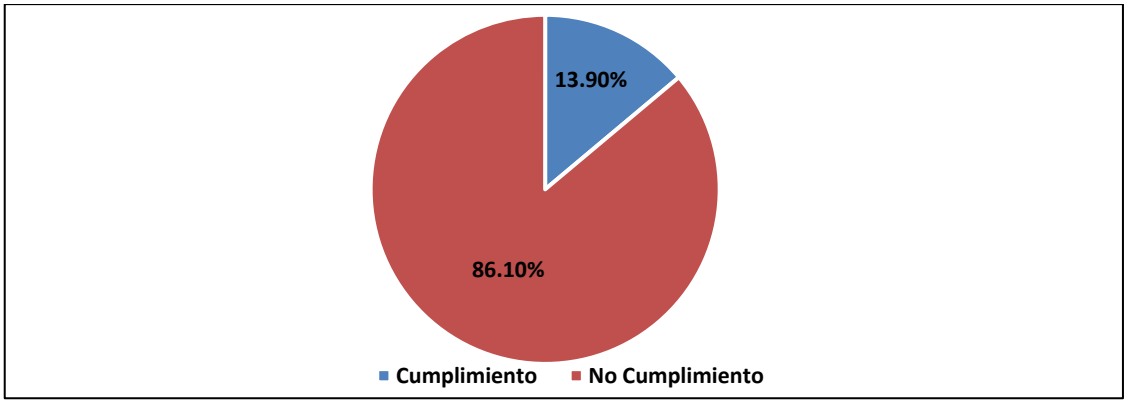


Figura 3.3. Proporción de cumplimiento de los puntos 4 al 10 de la Norma ISO 27001:2013. Fuente: Datos generados en el estudio

Estos requisitos son específicos y obligatorios, por lo cual, para que se pueda asegurar la completa implementación de la norma todos deben estar cubiertos. Con respecto al contexto de la organización, destaca la falta de ejecución de un método de control, además que en la institución, la totalidad del personal desconoce qué papel juegan dentro del sistema de gestión que se logre implementar, por lo que se observa la necesidad de que se asuma la implementación de in SGSI y que este logre establecerse de manera adecuada, lo cual, contempla que todo el personal conozca su papel como generador o controlador/mitigados de las brechas de seguridad y riesgos.

En el caso del aparatado de liderazgo, se observó que a pesar de existir una estructura orgánica firme con roles definidos, se desconoce completamente los riesgos que pueden generar a la institución la falta de controles de los activos de la información, por lo que, es de esperar, como en efecto ocurre, que no existan políticas de seguridad ni se conozca el papel de cada quien, situación que soporta la falta de conocimiento de las obligaciones del personal con respecto a la SI que se observó en el contexto de la organización. En este sentido, se hace necesario que se creen políticas internas considerando la SI como elemento importante en la integridad operativa de la unidad educativa, esto, se puede reforzar, al momento en que la institución asuma dicha responsabilidad y opte por readaptar las políticas operativas existentes a la consecución de objeticos asociados a la SI.

Al respecto de la planificación, evidentemente, al no existir un sistema de gestión, o peor aún, al no conocerse en la institución el alcance e importancia del control de los

activos o minimización de los riesgos, no existen ninguno de dichos elementos evaluados, esta situación, puede ser solventada con la implementación de un SGSI ya que este contiene.

Esta situación, es similar a la observada en la evaluación de los elementos de soporte, operaciones, evaluaciones de desempeño y mejoras, es decir, no existe y se desconocía de la importancia de los SGSI y, por lo tanto, no hay soportes documentales de estos.

3.5. Verificación de los requisitos indicados en el anexo a de la norma ISO 27001:2013

Tal como se indicó en el apartado anterior, fue necesario la verificación del cumplimiento de los elementos normativos que se disponen en el Anexo ‘A’ (2014) de la norma ISO 27001:2013. Para esto, se realizó una verificación por medio de un Check list, en el cual se incluyen todos los apartados estipulados en el respectivo documento (ISO 27001:2013.

Esta lista de verificación, igualmente es adecuada como modelo para seguir luego de la implementación del SGSI para realizar seguimiento y control de los estándares a los que la institución se adapta (ver anexo 13 para observar los resultados completos).

En la Figura 3.4, es posible observar que en la institución educativa evaluada, a pesar de posees varios aspectos adaptaos a los requerimientos de la norma ISO 27001:2013 que se indican en el Anexo A de dicha norma, todavía existe un alto porcentaje de inadecuación que sobrepasa el 79%.

Principalmente se observa la carencia de las documentaciones estándares requeridas en la norma en diversos de sus apartados. Otros elementos en los que se observan carencias importantes corresponden a los procedimientos estándares ante diversas situaciones afines con la SI, sin embargo, a pesar de las fallas mostradas en esta evaluación de cumplimiento, la situación es reversible si se asume la implementación de un SGSI como el que se plantea en este estudio.

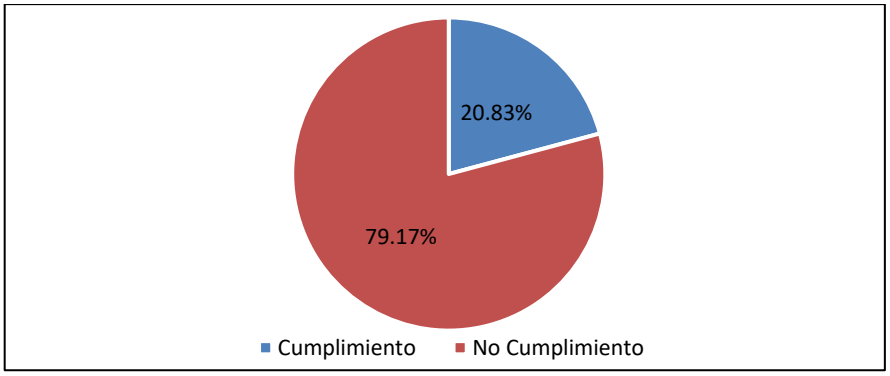


Figura 3.4. Proporción general de cumplimiento con los indicativos aplicables a la institución que consta en el ANEXO A de la norma ISO 27001:2013. Datos generados en el presente estudio

3.6. Validación real de riesgos y amenazas de los activos informáticos por medio del método MAGERIT

Luego dela implementación de los pasos anteriores, se procedió a la valoración real de los riesgos y amenazas mediante la metodología MAGERIT creada por el CSAE (2012a). En particular, esta metodología se basa en la implementación de un proceso de dos pasos, siendo el primero la calificación estandarizada de los riesgos a los que se enfrentan los activos de la información y la segunda, contempla la definición de acciones necesaria para contrarrestar los riesgos observados (CSAE, 2012a). Para esto, partiendo del inventario de activos generados, se realiza una valoración de los mismos basándose en la identificación de las amenazas, estas, según dicha metodología se clasifican como: Desastres naturales, "De origen Industrial, Errores y fallos no intencionales y ataques intencionales" (CSAE, 2012a, pág. 27) (Ver Anexo 1).

Seguidamente, según lo estipula la metodología empleada, las amenazas asociadas a cada activo, deben ser valoradas en base a la frecuencia con la que podrían ocurrir los sucesos que alteren la integridad de los activos, a los cuales, se le asigna una puntuación que se encuentra tabulada (Ver Anexo 2). Posteriormente, se realiza con estos datos la valoración del riesgo potencial, con la cual, se establece que los niveles de riesgo aumentan en base al impacto del daño en el activo y la frecuencia con la que esta ocurra, dicha valoración se corresponde a: $\boldsymbol{Riesgo = Probabilidad\ x\ Impacto}$ (CSAE, 2012a, pág. 28).

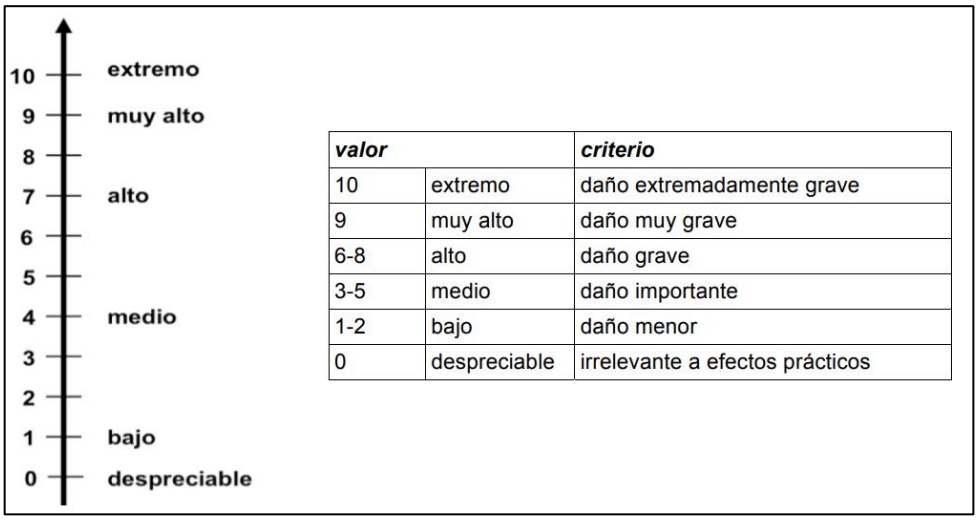
La interpretación y análisis de esta valoración se facilita mediante el empleo de la curva de valoración que se muestra en el anexo 3, misma que permite distinguir cuatro zonas de riesgo (Tabla 9), en base a las cuales se deben asumir determinados tipos de salvaguardas (ver Anexo 4) para asegurar la integridad de los archivos de información según el nivel de riesgo observado (ver Anexo 5).

Tabla 9. ***Zonas de riesgo en la valoración de amenazas a través del método MAGERIT***

Zona	Interpretación	Categorización
Zona 1:	Riesgos muy probables y de muy alto impacto	MA (Críticos)
Zona 2	Riesgos que varían desde situaciones improbables y con impacto medio hasta situaciones muy probables, pero de impacto bajo o muy bajo	M (Apreciables)
Zona 3	Riesgos improbables y de bajo impacto	MB, B (Despreciables o bajos)
Zona 4	Riesgos improbables, pero de muy alto impacto	A (Importantes)

Fuente: CSAE: (2012a, pág. 28) Diagramado y adaptado por el Autor.

Seguidamente, los activos presentes fueron codificados basándose en las indicaciones de la metodología MAGERIT en su Libro II (2012b, págs. 8-13) (Ver Anexo 6). La escala de valoración utilizada posee 10 valores adjudicables (CSAE, 2012b, pág. 19), en el cual, 0 es el valor o nivel más bajo de riesgo (Figura 3.5 y 3.6).



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Figura 3.5. Criterios de Valoración. Recuperado de (CSAE, 2012b, pág. 19)

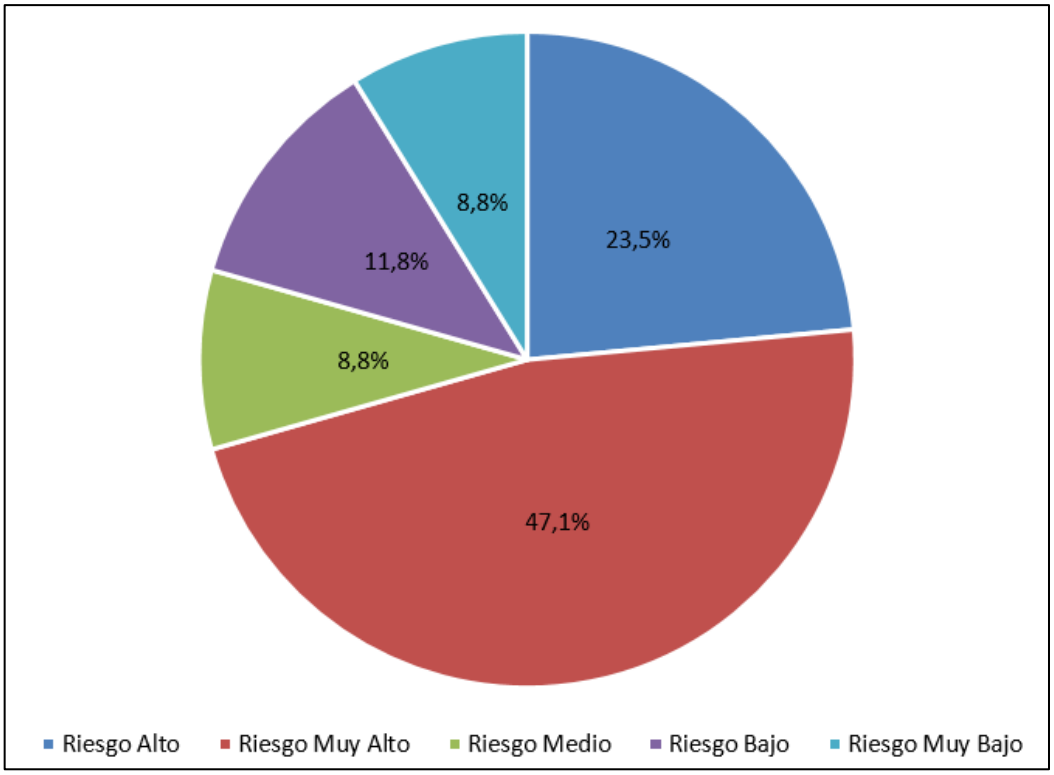


Figura 3.6. Resultados de la valoración de riesgo. Resultados del estudio. La tabla completa se encuentra en el anexo 11.

Como se observa en la figura 3.6, la unidad educativa adventista “Gedeón” posee una gran cantidad de elementos de riesgo que pueden incidir negativamente en la seguridad de los activos de la información, con lo cual, deben asumirse acciones rápidas para mitigar estas situaciones. Sin embargo, estos elementos mayoritariamente se asocian al mantenimiento del *hardware* y a las redes, por lo que estas adecuaciones deben ser minuciosas y prepararse con detalle para que su implementación sea correcta.

Otro elemento destacable en cuanto a riesgo, es la posible filtración de información por la falta de controles pertinentes y adecuados con respecto al acceso que puede darse a los elementos de la información por las distintas vías observadas, en estos casos, la información no es encriptada correctamente ni las computadoras poseen los resguardos de acceso más adecuados, sin mencionar la inexistencia de protocolos y directrices orientados a proteger estos activos.

Por su parte, los softwares computacionales de procesamiento de texto , a pesar de representar un riesgo baja, representan un brecha de seguridad importante debido a que estos no cuentan con licencias originales activas y son además, por así decirlo, algo

obsoletos, adicionalmente, muchas de las PC, no cuentan con antivirus, esto particularmente se observa en las computadoras de la sala de computación, mismas, que se encuentran integradas en la red de la institución, y a la cual tienen acceso todos los estudiantes y no se toman previsiones para su adecuado uso o respaldo.

Una solución inmediata a esta situación es la de la actualización de los dispositivos en cuestión, tanto a nivel de hardware como de software, igualmente, a pesar que la unidad educativa se encuentra en una región con un alto potencial de eventos sísmicos y volcánicos, los riesgos de origen natural no representan mayor problema de seguridad debido a que las instalaciones de la institución son relativamente modernas y esta adecuada para soportar estos incidentes naturales, o a menos los sísmicos, pero los eventos volcánicos se encuentran fuera de rango para ejercer un efecto notablemente negativo más allá que los estragos que pudieran ocasionar la acumulación de cenizas de presentarse una situación como esta.

CAPÍTULO 4. IMPLEMENTACIÓN

4.1. Desarrollo de la propuesta de implementación (Presentación)

Debido a la dinámica propia de toma de decisiones dentro de la institución, la cual, pasa por un consejo directivo en la unidad educativa y depende de los aportes y las directrices finales de la Asociación Adventista a la que está adscrita, implican que se presente una propuesta de manual de implementación que facilite la vía para la toma de decisiones, además, que reduce el trabajo que debe realizar los implementadores para obtener resultados acordes a los objetivos de seguridad que se requieren alcanzar.

En este sentido, esta sección, si bien no se constituye de manera formal como un manual dado que el mismo debe ser aprobado por los actores antes mencionados, presenta la base documental principal para el establecimiento definitivo del mismo en el momento que este sea requerido. Por tal motivo, los acápites siguientes se presentan en el orden que debe tener el manual de procedimientos para el aseguramiento del funcionamiento adecuado de un sistema de gestión basado en la norma ISO 27001:2013.

4.1.1. Propósito de la propuesta

La finalidad del presente planteamiento se centra en generar una propuesta de implementación viable de un SGSI basado en la norma ISO 27001:2013, con la cual, la Unidad Educativa Adventista Gedeón, pueda hacer frente a los riesgos y vulnerabilidades detectados en los activos de la información analizados en los acápites previos.

4.1.2. Razones que motivan el diseño de la propuesta

La razón primordial para la ejecución del presente proyecto de investigación es la de solventar la falta de seguridad que padecen los activos de la información dentro de la unidad educativa.

Esta es una institución que, si bien no es tan grande como otras que se pueden encontrar en la ciudad de Quito, Pertenece a una red de instituciones de envergadura internacional, y que puede ser objeto de vulneraciones, tanto en sus activos como en la reputación de la institución global, además, son los datos de estudiantes y representantes que pueden ser objeto de hurto para emplearlos con fines ilícitos.

Adicionalmente, la propuesta busca convertirse en un inicio para la ejecución definitiva y futura de un sólido SGSI, que incluso, pueda optar por la respectiva certificación.

Por su parte, el entorno en el que funciona este tipo de institución, implica que constantemente se estén generando y manipulando información que puede ser sumamente sensible para diversos actores de varios Stakeholders, asúmase como tales, a los datos privados de alumnos, padres y representantes, docentes, y la misma institución y sus entes directrices (Grupo Adventista), adicionalmente se manejan calificaciones de alumnos; por todo esto, la institución debe garantizar la protección de la información que maneja a través de la aplicación de políticas y procedimientos que aseguren el cumplimiento de este estándar de inviolabilidad de la privacidad, lo cual, se logra asumiendo posturas y acciones que eliminan, disminuyen y/o controlan el uso y acceso a los activos de la información.

4.2. Objetivos de la propuesta de implementación

La presente propuesta de implementación posee los siguientes objetivos estratégicos, direccionales y operativos:

1. Consolidar una propuesta aplicable de SGSI sustentado en la norma ISO 27001:2013.

2. Generar la base procedimental que garantice el adecuado manejo, valoración y control de los activos de la información pertenecientes a la unidad educativa
3. Establecer los lineamientos para detectar los elementos de seguridad, las vulnerabilidades y amenazas más críticos en la unidad educativa.

4.3. Alcance del SGSI

4.3.1. Propósito, alcance y usuarios

La propuesta que se muestra en esta investigación, es aplicable a todos los elementos de la información que se generen dentro de la unidad educativa, así como también, al espacio físico de la institución y a los distintos actores humanos que estén relacionados con dichos activos.

4.3.2. Grado real de ajuste a la norma

Las evaluaciones preliminares que en esta investigación se incluyen, representan una vista actualizada de la situación de SI en la que se encuentra la institución, sin embargo, por ser una propuesta que depende de la institución para su implementación la adecuación a la norma, al momento de instaurar la misma debe ser medida nuevamente, en toda oportunidad donde se reevalúe la misma, debe realizarse una nueva evaluación donde se verifique el grado actual de cumplimiento de la normativa, par esto, se requiere que la unidad educativa, cree una comisión que asuma el trabajo de implementación (en un principio), y de evaluación (para los casos de evaluación o auditoria futura del SGSI) y para entonces se realice una nueva valoración en base a los dispuesto en esta propuesta.

4.3.3. Duración y estructura del proyecto

Dadas las características observadas en la evaluación preliminar y a las restricciones operativas que solo pueden ser subsanadas por la vía administrativa de la institución, esta investigación, de momento, alcanza el nivel de propuesta de implementación, por lo cual, no es posible establecer un tiempo mínimo para la implementación, debido a que, como ya se mencionó, depende de la junta directiva de la institución, establecer los recursos requeridos para la adquisición de los elementos informáticos que formaran parte de los

correctivos o la adecuación de los espacios para que los elementos asociados con la información (sus activos) estén más resguardados.

En el caso de la implementación del SGSI, esta debe ser implementada en un periodo que en primera instancia, no exceda de los seis meses calendarios, esto debido a que son diversos los aspectos que deben cumplirse, luego de implementada, y de requerirse reajustes a los procedimientos y controles, los mismos deben ser implementados en un periodo no mayor de dos meses debido a que la gran mayoría de los elementos de seguridad ya se deben encontrar activos y funcionando, esto, es responsabilidad de la comisión de seguimiento y control del SGSI que se a establecida por la institución.

4.3.4. Responsabilidades

La implementación del SGSI que se propone, será realizada por parte de la junta directiva de la institución, esta, tras recibida la propuesta debe decidir la asignación del presupuesto pertinente, programar las comprar necesarios y planificar la ejecución del mismo sin que esto intervenga en las funciones ordinarias de la institución.

Luego de un año de implementado el SGSI y posterior a su primera auditoria, los correctivos que fueran necesario implementar, como se mencionó en la sección anterior, son responsabilidad de la comisión de seguimiento y control del SGSI que se cree para tal fin.

4.3.5. Recursos

Los recursos empleados en la generación de la propuesta, son de carácter técnico y humano. Entre los elementos de orden humano relacionados con la propuesta, se encuentran todos los stakeholders de la institución que estén de alguna manera relacionados con alguno de los activos de la información. Así mismo, se encuentra el personal técnico capacitado que debería contratase para que se haga cargo de la sección de informática, y del mantenimiento y control del SGSI que se propone. Por su parte, los elementos técnicos, están representados en los softwares y hardwares que se emplearan para el procesamiento de la información que se genere, adicional al material bibliográfico

de referencia y normativo que es indispensable para la adecuada orientación de las acciones a seguir.

4.4. Control y propiedad del presente manual

Este documento, junto a todos los que se generen a partir del mismo, son propiedad exclusiva de la Unidad Educativa Gedeón, por lo que queda totalmente prohibida su reproducción, distribución no autorizada o copia del mismo sin que esto sea previamente autorizado por la directiva del plantel.

4.5. Términos y definiciones

Las definiciones son necesarias para estableces un idioma común, en este caso, es necesario establecer de manera clara cuales son los términos que se emplearan a lo largo de la implementación del SGSI o cuando se haga referencia a este para que así, todas las personas relacionadas con el mismo entiendan de que se está hablando.

En este sentido, se establece que todas las definiciones técnicas empleadas son las que establece la Organización Internacional de Normalización (ISO por sus siglas en Ingles) en la web de documentación que se indican a continuación y en la misma norma ISO 27000 (2018). La web de las definiciones asociadas a la norma ISO y en la cual se fundamenta la presente propuesta es la siguientes: http://www.iso27000.es/glosario.html

4.6. Compromiso de la dirección

En esta sección, se deja constancia del compromiso de la junta directiva de la Unidad Educativa Gedeón con el establecimiento y mantenimiento de altos estándares en la Seguridad de la Información tras asumir, de manera total e integra los principios que para tal fin se exponen en la Norma ISO 27002, misma que describe los controles y los objetivos de control para la SI. Se compromete de esta manera, con la salvaguarda oportuna y adecuada de sus activos de información por medio de la protección de estos de las amenazas que puedan afectarle. Lo cual se logrará por medio de la adecuada gestión del riesgo, el cumplimiento de requisitos legales, mejores prácticas e implementación de controles.

4.7. Planificación del SGSI

Para la adecuada implementación del SGSI se establece el seguimiento obligatorio de las siguientes etapas, mismas que corresponden al ciclo de Deming:

- Documentar la situación actual por medio de la valoración de dichas condiciones y la respectiva documentación de la situación
- Implementación del SGSI
- Evaluación mediante auditorías internas y externas
- Mejoramiento continuo del SGSI en base a os resultados de las auditorias.

4.8. Requisitos del SGSI

El SGSI debe cumplir con todos los elementos aplicables al tipo negocio que se contemplen dentro de la norma ISO 27001:2013, los cuales son:

- Definición del alcance del Sistema de Gestión de Seguridad de la Información
- Definición de las políticas de seguridad
- Definición del método de evaluación y gestión del riesgo
- Identificación de los riesgos
- Valoración de las opciones y formas de afrontamiento de los riesgos
- Creación de la declaración de aplicabilidad de controles y requerimientos
- Impulso de un plan para el tratamiento de los riesgos
- Establecimiento de los controles
- Ejecución de actividades de formación sobre la SI

4.9. Documentación

Al final, y con el objeto de validar y garantizar la implementación del SGSI, la Unidad Educativa Gedeón debe poseer la siguiente documentación básica:

- Documento probatorio de la autorización y compromiso de la junta directiva con el establecimiento del sistema de gestión de la información
- Documento institucional donde se manifiesta el alcance del SGSI.

- Documento con las políticas del SGSI
- Documento referencial sobre la metodología de evaluación del riesgo a emplear en la implementación y evaluación del SGSI.
- Informes de las evaluaciones de riesgo.
- Plan para el abordaje de los riesgos detectados.
- Declaración de aplicabilidad (SoA).

4.10. Responsabilidad de del consejo directivo del SGSI

El establecimiento del SGSI requiere de la definición de roles y responsables del mismo, con lo cual, se pretende que todo el personal involucrado esté al tanto de su papel dentro del sistema de gestión.

Es fundamental definir roles y responsables para apoyar y cumplir la política de seguridad de la información, a continuación, se relacionan y describen. En primer lugar, se establece que el compromiso del ente director es el siguiente:

- Definir e instituir las políticas y objetivos de seguridad de la información más adecuados y divulgarlos a todos los stakeholders
- Garantizar la evaluación periódica del SGSI y la corrección de las no conformidades que se lograran detectar.
- Gestionar todos los aspectos administrativos y directivos relacionados con el SGSI de manera oportuna, así como hacer cumplir los roles y responsabilidades de todos los actores afines con este.
- Valorar y establecer los criterios de aceptación de determinados riesgos de SI.
- Promover en todos los actores, la aceptación de las normativas de seguridad implementadas.

Por su parte, se establece que los grupos de actores que están relacionados con la gestión de riesgos de SI son: la Directiva del SGSI, Los propietarios de los activos de la información y los usuarios de la información. Al respecto como se muestra en la tabla 4.1, estos tendrán las siguientes responsabilidades:

Tabla 10. ***Responsabilidades de los stakeholders***

Grupo de interés	RESPONSABILIDADES
Directiva del SGSI	Planificar, instituir, conservar, examinar, controlar y optimizar el SGSI en base a lo dispuesto en la ISO 27001:2013
	Administrar y comprobar los progresos y la eficacia del SGSI, asumiendo como indicadores a los objetivos y metas planteadas además del resultado de las auditorías.
	Cuidar que sean efectuadas las políticas, reglas y instrucciones de SI.
	Valorar y certificar las reglas, instrucciones, procesos y controles definidos para la SI.
	Verificar periódicamente la efectividad de las salvaguardas asumidas
	Dirigir y fomentar de manera activa los planes de capacitación de la SI en todos los stakeholders
	Garantizar la puesta en marcha y la efectividad del plan de continuidad de negocios cuando este requiera ser implementado
Propietario de activo de información	Catalogar la información en base a los niveles que para este fin establezca la directiva del SGSI al valorar la sensibilidad de los datos
	Definir los niveles de acceso que tienen las personas a la información que se genera en la institución.
	Genera las autorizaciones pertinentes para que los diversos usuarios puedan acceder a algún tipo de documento
	Establecer y vigilar el cumplimiento de los niveles de autorización de acceso a la información
	Mantener una revisión periódica de los estándares y controles de acceso que se implementan en la institución a los diferentes activos
	Vigilar que sea asegurada la integridad, confidencialidad y disponibilidad de la información
Usuarios de la información	Utilizar la información solo para los propósitos aprobados por la directiva del SGSI y el dueño de los activos de la información.
	Asumir buenas prácticas en cuanto al uso de la información, principalmente aquellas dictadas por la directiva del SGSI, en forma de políticas y directrices.
	Garantizar que cada violación de los protocolos de seguridad establecidos que detecten sean violados por otros, serán reportados oportunamente
	Utilizar los activos de la información solo para los fines establecidos y autorizados

4.11. Gestión de los recursos del SGSI

La directiva de la unidad educativa será quien canalice los recursos monetarios necesarios para la implementación del SGSI, luego de esto, será quien también asigne el presupuesto necesario para el mantenimiento del mismo previo análisis de las respectivas solicitudes realizadas por la dirección del SGSI, igualmente esta se compromete a contratar al personal calificado necesario para que los objetivos de seguridad se alcancen y se mantengan

4.12. Políticas de seguridad de la información

Las diversas políticas son de obligatorio cumplimiento por parte de todos los relacionados con la institución y todos aquellos terceros que puedan inferir directamente en la SI dentro de la unidad educativa, al efecto, en la sección de anexos (Anexo 14 en adelante) se encuentran las respectivas políticas.

4.12.1. Propósito, alcance y usuarios a los que se dirigen las politicas

Fundamentados en los resultados obtenidos en las valoraciones preliminares, la directiva de la Unidad Educativa Adventista Gedeón, como principal responsable de las actividades desarrolladas en la unidad educativa, en reunión directiva expondrá los hallazgos y alcances a su personal y a luego a todo tercero que en algún grado este asociado con la institución (representantes estudiantes o personal de la red adventista a la que pertenecen).

Esta reunión informativa debe ser sumamente explicita a la hora de indicar los riesgos de no tener un SGSI implementado y las ventajas que acarrearía para la institución la implantación del mismo, igualmente, deben dejar claro el papel y las responsabilidades de cada stakeholder en el tema de la seguridad de los activos informáticos. Roda esta información no debe ser entregada únicamente de manera verbal a las partes interesadas, sino, que adicional a la mencionada reunión, la directiva debe preparar un material gráfico didáctico con lo que formalmente queden expresados los propósitos, alcances, usuarios y la responsabilidad de cada uno de estos.

4.12.2. Estrategia de seguridad de la información

Las estrategias de SI que debe asumir la Unidad Educativa Adventista Gedeón, son única y exclusivamente los indicados en la normativa internacional ISO 27001:2013. Podrán de ser necesario implementarse controles adicionales definidos precisamente por la respectiva necesidad, pero nunca podrán ser menos o distintos a los indicados en la normativa. Esta estrategia, basado en las observaciones preliminares, mayoritariamente incluyen la creación de toda la documentación normativa y operativa faltante, adecuación de los elementos físicos necesarios y el seguimiento periódico de los controles.

4.12.3. Objetivos de las políticas de seguridad

De manera general, la implementación de políticas de SI en la institución, son las de salvaguardar los activos de la información, de manera que todos los datos se encuentres totalmente resguardados ante cualquier amenaza y garanticen así la integridad de la institución o de las personada de las cuales dicha información es de vital importancia. Para lograr esto, se plantean los objetivos indicados en la Tabla 11, los cuales se corresponden con los objetivos planteados para cada uno de los dominios que abarca la normativa ISO 27001:2013.

Tabla 11. ***Objetivos específicos del SGSI propuesto basado en los dominios indicados en la Norma ISO 27001:2013***

Dominio	Objetivos de control
Política de seguridad	Proporcionar dirección de gestión y soporte para la SI de acuerdo con los requisitos comerciales y las leyes y regulaciones relevantes
Organización de la SI.	Gestionar la SI dentro de la organización. Mantener la SI de la organización y las instalaciones de procesamiento de información a las que acceden, procesan, comunican o administran terceros.
Gestión de activos	Implementar y mantener la protección adecuada de los activos de la organización. Garantizar que la información reciba un nivel adecuado de protección.
Seguridad de recursos humanos	Garantizar que los empleados, estudiantes, representantes u otros usuarios externos comprendan sus responsabilidades y conozcan los roles y responsabilidades de cada uno, y de esta manera reducir el riesgo de robo, fraude o mal uso de las instalaciones. Garantizar que todos los empleados, estudiantes, representantes u otros usuarios externos conozcan las amenazas y preocupaciones de SI, sus responsabilidades y responsabilidades, y estén equipados para respaldar la política de seguridad de la organización en el curso de su trabajo normal y así reducir el riesgo de error humano. Garantizar que los empleados, estudiantes, representantes u otros usuarios externos salgan de la institución educativa o cambien de empleo de manera ordenada.
Seguridad física y ambiental	Evitar el acceso físico no autorizado, daños e interferencias a las instalaciones y la información de la organización. Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las actividades de la organización.
Gestión de comunicaciones y operaciones.	Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. Implementar y mantener el nivel adecuado de SI y prestación de servicios en línea con los acuerdos de prestación de servicios de terceros. Minimizar el riesgo de fallas del sistema. Proteger la integridad del software y la información. Mantener la integridad y disponibilidad de la información y las instalaciones de procesamiento de información. Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte. Evitar la divulgación no autorizada, modificación, eliminación o destrucción de activos, y la interrupción de las actividades de la institución. Mantener la SI y el software intercambiados dentro de una organización y con entidades externas.

	Mejorar la detección de actividades de procesamiento de información no autorizadas.
Control de acceso	Controlar el acceso a la información. Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas de información. Evitar el acceso no autorizado de usuarios, el compromiso o el robo de información y las instalaciones de procesamiento de información. Evitar el acceso no autorizado a servicios en red. Evitar el acceso no autorizado a los sistemas operativos. Evitar el acceso no autorizado a la información contenida en los sistemas de aplicación. Garantizar la SI cuando se utilizan las instalaciones de computación móvil y teletrabajo.
Adquisición, desarrollo y mantenimiento de sistemas de información.	Garantizar que la seguridad sea una parte integral de los sistemas de información. Evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones. Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos. Garantizar la seguridad de los archivos del sistema. Mantener la seguridad del software y la información del sistema de aplicación. Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.
Gestión de incidentes de SI.	Garantizar que los eventos de SI y las debilidades asociadas con los sistemas de información se comuniquen de manera que se puedan tomar medidas correctivas oportunas. Garantizar un enfoque coherente y efectivo se aplica a la gestión de incidentes de SI.
Gestión de la continuidad del negocio	Contrarrestar las interrupciones en las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes de los sistemas de información o desastres y asegurar su reanudación oportuna.
Conformidad	Evitar incumplimientos de cualquier ley, obligación legal, reglamentaria o contractual, y de cualquier requisito de seguridad. Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional. Maximizar la efectividad y minimizar la interferencia hacia / desde el proceso de auditoría de los sistemas de información.

Fuente: Diagramado por el autor.

4.12.4. Políticas de seguridad de los activos de la información

Para cumplir con este apartado en la implementación de la propuesta del SGSI, se generaron una serie de políticas básicas asociadas a las carencias detectadas, mismas que se proponen sean efectuadas como parte del proceso de implementación del sistema de gestión que se propone (***Tabla 12***):

Tabla 12***. Delimitación de las políticas propuestas para la seguridad de los activos de la información.***

Política	Indicación
Política de seguridad normal	Se requiere que la totalidad del personal docente, administrativo, tercerizado, alumnos y representantes, resguarden todos y cada uno de los activos de la información de la institución. Con lo cual, es directa y contundente la prohibición de la reproducción, manejo o uso a cualquier nivel de la información que pueda considerarse sensible para los intereses de la institución y de cualquiera de las partes interesadas. En este sentido, toda documentación o activo de la información. Podrá ser empleado por las partes mencionadas en consonancia con las autorizaciones respectivas emitidas por la institución o en base a las actividades normales de esta, siempre y cuando dicha información o activo generado o usado, no socave la seguridad del SGSI. Esta política abarca e incluye el maltrato o destrucción accidental o intencional de cualquiera de los activos informáticos propiedad de la institución educativa.
Política de la SI general	Serán generadas e implementadas una serie de normativas y procesos de obligatorio cumplimiento que apunten sin excepción al resguardo adecuado y seguro de la información sensible que se encuentra a cargo de la institución, como lo son (Pero no limitados a estos): datos de alumnos, empleados, empresas tercerizadas, generadoras de servicios de valor agregado, distribuidores, docentes, representantes, personas o instituciones de la red adventistas, entre otros. Esta política está orientada al aseguramiento de la integridad, disponibilidad y confiabilidad de la información que la institución posee.
Política de la gestión del riesgo	Serán generados e implementados con carácter de obligatoriedad y sin ningún tipo de excepción, manuales operativos de manejo y control de riesgos.
Política de la protección de datos	Se aplicaran controles según el tipo de usuario de la información
Política de auditoría	Se programaran auditorias anuales relacionadas con el control de procesos y activos informáticos y de la información, en los mismos, se priorizara la verificación de cumplimiento de los procesos y las políticas que acá se indican y establecen.
Política de calidad	Como garantía de la calidad en el manejo de la información, y como parte de un proceso de mejora continua, la institución, representada por su junta directiva, asumen la responsabilidad, el deber y la obligación de redefinir las políticas actuales cada vez que se detecten oportunidades de mejoras de las mismas, si esto no ocurriera en un periodo mínimo de un año, en cada proceso de auditoria se verificara la posibilidad de asumir acciones que no se hayan implementado y que sumen a la SI.
Política de los dispositivos traídos por el usuario	Con la intensión de que no sean esparcidos dentro de red de la institución softwares maliciosos, todo el personal, administrativo, docente y alumnos, tienen estrictamente prohibidos el empleo de dispositivos personales (Principalmente computadoras, pero no limitadas a estas) conectándolos a la red de la unidad educativa. Para poder hacer uso de estos dispositivos, la persona interesada debe contar con la autorización de la directiva, y esta, solo puede ser emitida si el equipo en cuestión se encuentra configurado con los mismos estándares de seguridad informático que el resto de los activos de la unidad educativa. En caso contrario, solo los profesores tienen autorización de empleo de sus computadores personales pero los mismos, no podrán ser conectados bajo ninguna modalidad o excepción a la red. Los estudiantes, SOLO CUANDO SEA ESTRICTAMENTE NECESARIO Y BAJO LA AUTORIZACVION DE PROFESOR RESPONSABLE, podrán usar sus computadoras personales, pero sin poderlas conectar a la red. Se prohíbe el uso de memorias USB en los dispositivos de la institución para cualquier persona si no se genera previamente un cheque de seguridad

	con un software antivirus actualizado, con licencia activa, y que sea propiedad de la institución.
Política de la instalación de *software* y *hardware*	Queda prohibido que cualquier persona instale o desinstale cualquier tipo de software o hardware de las computadoras de la institución, para que esto ocurra debe estar justificado la necesidad del mismo, y este proceso lo llevara a cabo una personas¿ especializada en el tema y designada para tal fin por la junta directiva
Política de la comunicación institucional	Se establecerá un servicio de correo electrónico institucional, con soporte actualizado de antivirus, y solo por esta vía, se transmitirá la información institucional. Queda prohibido el envío de información de la institución o relacionada con ella a cualquier persona que no posea dicho correo. Las cuentas serán generadas por el personal técnico que se disponga para este fin, y serán estos mismos, los que inmediatamente de la baja de algún miembro empleado de la institución, eliminen el usuario, en otras palabras, al momento que un empleado deje la institución, inmediatamente debe ser dado de baja del servicio de correo electrónico
Responsabilidad	Todo el personal, o miembro de la institución independientemente del tipo de relación que posea con la misma. Deberá responsabilizarse automáticamente por los perjuicios que sufran los activos cuando estén a su resguardo. El no cumplimiento de este requerimiento, autoriza expresamente a la dirección de la unidad educativa a que tome las medidas correctivas o sancionatorias pertinentes.
Procedimientos en incidentes de seguridad	Cada vez que ocurra una incidencia con alguno de los activos de la información, se está obligado sin excepciones a informar del mismo a la directiva, y la directiva se encuentra obligada a garantizar el levantamiento de un informe técnico donde se incluyan detalles de interés y recomendaciones para limitar o eliminar el riesgo de ocurrencia de estos eventos, así mismo, la directiva está obligada que en el periodo de un mes, se asuman y realicen los correctivos que consten en las indicaciones incluidas en el informe de la incidencia

Fuente: Diseñado por el Autor.

4.13. Métodos de análisis y evaluación y reporte de riesgos.

4.13.1. Propósito, alcance y usuarios.

El propósito expedito del análisis y evaluación de la SI es el de lograr determinar de manera periódica la existencia de brechas de SI en la institución.

Este abarcara el análisis periódico de activos informáticos (actualización de los inventarios existentes), determinación de riesgos y amenazas, por medio del método MAGERIT. Para esto, se emplearán los manuales respectivos previamente documentados y citados en esta investigación, y se tomara come referencia los anexos que acá se incluyen y a la evaluación preliminar realizada. Todo el personal en responsable de informar los aspectos que le competan al momento del levantamiento de esta información, y es la Junta directiva de la institución la encargada y responsable de contratar al personal calificado para la ejecución de esta tarea.

4.13.2. Metodología de análisis evaluación de riegos y reporte de evaluación de riesgos.

Como se indicó previamente, el método de análisis de riesgos y vulnerabilidades que se propone es el representado en la metodología MAGERIT (*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)* creado por el CSAE (*Consejo Superior de Administración Electrónica*) (2012a).

4.14. Declaración de aplicabilidad.

4.14.1. Propósito, alcance y usuarios.

El propósito de la declaración de aplicabilidad es la de establecer los controles y la forma de aplicación de cada uno de estos dentro de la Unidad Educativa Adventista Gedeón. Estos controles, están basados en las fallas detectadas en la evaluación inicial y cada uno de ellos representa a cada uno de los elementos de seguridad establecidos en el Anexo A de la Norma ISO 27001:2013.

4.14.2. Aplicabilidad de controles

A continuación se muestran solo los controles establecidos en la norma ISO 27001:2013 que pueden ser aplicados, así mismo se muestra como debe ser este proceso (***Tabla 13***):

Tabla 13. ***Controles aplicables***

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
A.5 (Políticas de SI)	A.5.1 (Dirección de la gerencia para la SI)	A.5.1.1	Políticas para la SI	Las políticas de la SI deben ser redactadas de acuerdo a los objetivos y alcances previamente establecidos en este documento, así mismo, deben ser documentados adecuadamente y transferidos a todo el personal asociado a la institución a los cuales competa su aplicación
		A.5.1.2	Revisión de las políticas para la SI	Todas las políticas generadas deben ser revisadas y reevaluadas de manera periódica, sin que la revisión anual realizada en las auditorias respectivas del SGSI menoscaben la importancia de realizar alguna revisión adicional a la asociada al proceso mismo de auditoria. Los responsables de las revisiones son la directiva de la institución, el personal técnico especializado que se encarga del sistema de gestión y todo el personal que sea designado para esta labor. Los cambios detectados deben ser documentados y justificados.
A.6 (Organización de la SI)	A.6.1 (Organización Interna)	A.6.1.1	Roles y responsabilidades para la SI	Deben documentarse y socializarse los roles y responsabilidades de la SI definidos previamente.
		A.6.1.2	Segregación de funciones	Deben documentarse y socializarse la segregación del personal por áreas y definirse documentarse y socializarse las funciones de cada uno, estos solo deben tener acceso a los activos estrictamente necesaria para la realización de su trabajo.
		A.6.1.3	Contacto con autoridades	La dirección de la institución como encargada del proceso de implementación del SGSI o el personal técnico especializado contratado para tal fin, deben tener un contacto permanentemente actualizado con las autoridades, empresas o personas que puedan ayudar a mitigar algún evento de seguridad cuando este ocurriera.
		A.6.1.4	Contacto con grupos especiales de interés	
		A.6.1.5	SI en la gestión de proyectos	La directiva del plantel en la figura de su consejo de dirección será la encargada de dirigir y controlar el sistema de gestión, esta función, puede ser relegada a un o algunos terceros que la misma comisión escoja para tal fin.
	A.6.2 (Dispositivos móviles y trabajo a	A.6.2.1	Políticas de dispositivos móviles	Se debe documentar y distribuir la política de seguridad creada para el uso de dispositivos móviles en la institución
A.7 (Seguridad de los recursos humanos)	A.7.1 (Antes de asumir el empleo)	A.7.1.1	Selección	El personal debe ser escogido en función de su perfil.
		A.7.1.2	Términos y condiciones del empleo	Los aspectos relacionados con la SI deben ser incluidos en los contratos firmados por la institución y los empleados.
	A.7.2 (Durante la	A.7.2.1	Responsabilidades de la gerencia	La directiva debe declarar públicamente su comprensión sobre la importancia de la implementación del SGSI, y de esta manera dar inicio a la implementación formal del mismo.

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
		A.7.2.2	Conciencia, educación y capacitación sobre la SI	Deben establecerse cronogramas de trabajo para la formación de todos los Stakeholders con respecto a el SGSI que se implementara, en el cual, se hará hincapié en las funciones y responsabilidades de cada parte.
		A.7.2.3	Proceso Disciplinarios	Deben aplicarse sanciones a las partes interesadas que incumplan las disposiciones de seguridad del SGSI
	A.7.3 (Terminación y cambio de empleo)	A.7.3.1	Terminación o cambio de responsabilidades de empleo	El personal reasignado o dado de baja por cualquier motivo de la institución debe tener una pronta reasignación y baja (según sea el caso) de los accesos correspondientes a los activos de la información
A.8 (Gestión de activos)	A.8.1 (Responsabilidad por los activos)	A.8.1.1	Inventario de activos	El encargado del SGSI debe realizar inventarios periódicos de los activos de la información
		A.8.1.2	Propiedad de los activos	Debe definirse y documentarse la asignación de cada activo
		A.8.1.3	Uso aceptable de los activos	Los empleados o usuarios de los activos deben comprender y comprometerse a usar a los activos en base a lo establecido en los objetivos de seguridad
		A.8.1.4	Retorno de activos	Se mantienen registros de la devolución de los activos prestados a cualquier ente o persona
	A.8.2 (Clasificación de la Información)	A.8.2.1	Clasificación de la Información	Cada activos debe poseer una codificación que defina el nivel de clasificación de la información que contiene
		A.8.2.2	Etiquetado de la información	Cada uno de los activos debe estar marcados con la clasificación de la información asociada.
		A.8.2.3	Manejo de activos	Los activos deben ser manejados de acuerdo a la relevancia de la información que poseen
	A.8.3 (Manejo de medios)	A.8.3.1	Gestión de medios removibles	Debe implementase y difundirse la política descrita de uso de elementos removibles
		A.8.3.2	Disposición de medios	Los medios removibles propiedad de la institución deben ser almacenados, o destruidos (si es el caso de daño irreparable), de la manera más adecuada, evitando siempre que cualquier elemento de la información sea adquirido por terceros no autorizados.
A.9 (Control de acceso)	A.9.1 (Requisitos del negocio para	A.9.1.1	Política de control de acceso	Deben documentarse en las políticas de seguridad establecidas, las sub políticas para el control de acceso a los dispositivos y a la información

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
		A.9.1.2	Acceso a redes y a servicios de red	Las redes deben segmentarse y estableces una única red interna para los procesos administrativos a los cuales ni profesores ni alumnos tengan acceso
	A.9.2 (Gestión de acceso de usuarios)	A.9.2.3	Gestión de los derechos de acceso privilegiado	Se deben crear perfiles de usuario para acceso a los computadores de acuerdo al nivel de información que estos puedan manejar, y en base a los mismos se regulara el acceso a los activos de información.
		A.9.2.4	Gestión de información de autenticación secreta de usuarios	Se deben entregar personalmente a cada interesado las claves de acceso a los dispositivos a los que puedan ingresar, igualmente, la inclusión a la red será realizada exclusivamente por el personal autorizado para tal fin y por los medios que se dispongan para esto
		A.9.2.5	Revisión de los derechos de acceso de usuarios	Se debe revisar de forma periódica que los accesos asignados a cada usuario son los correctos y no pertenecen a terceros. Toda eventualidad debe ser documentada
		A.9.2.6	Remoción o ajuste de derechos de acceso	Al personal que salga de la institución debe serle retirado los accesos a los sistemas informáticos
	A.9.3 (Responsabilidades de los usuarios)	A.9.3.1	Uso de información de autenticación secreta	La información de acceso asignada debe ser confidencial e intransferible
	A.9.4 (Responsabilidades de los usuarios)	A.9.4.1	Restricción de acceso a la información	Los derechos de acceso deben ser asignados en dependencia de la información que puede manejar cada parte interesada
		A.9.4.2	Procedimiento de ingreso seguro	Los dispositivos informáticos deben tener protegido el acceso y la información debe ser cifrada
		A.9.4.3	Sistema de gestión de contraseñas	Se implementaran mecanismos de recuperación de contraseñas de forma automática y todos deben respetar las políticas de seguridad relacionadas con este tema
		A.9.4.4	Uso de programas utilitarios privilegiados	Los softwares que sean necesarios únicamente son los autorizados a instalas en los respectivos dispositivos computacionales
		A.9.4.5	Control de acceso a códigos fuente de los programas	Deben asumirse los controles necesarios para asegurarse que los softwares no se encuentren corruptos
A.10. (Criptografía)	A.10.1 (Controles Criptográficos)	A.10.1.1	Política sobre el uso de controles criptográficos	Deben establecerse lineamientos criptográficos apropiados para los elementos informáticos de la institución.
		A.10.1.2	Gestión de claves	Debe documentarse las políticas asociadas al tiempo de vida de las claves criptográficas y periódicamente revisar el cumplimiento de la misma
A.11 (Seguridad	A.11.1 (Área	A.11.1.1	Perímetro de seguridad física	Debe modernizarse el sistema de control de acceso físico, se recomienda el empleo de datos biométricos o tarjetas electrónicas para así restringir y controlar el acceso a áreas de seguridad de nivel variado

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
		A.11.1.2	Controles de ingreso físicos	
		A.11.1.4	Protección contra amenazas externas y ambientales	Debe actualizarse el plan de continuidad de negocios cada vez que sea necesario.
		A.11.1.6		
	A.11.2 (Equipos)	A.11.2.1	Emplazamiento y protección de los equipos	Los activos informáticos deben estar protegidos en la medida de las posibilidades de las amenazas físicas, por lo cual, deben documentarse y difundirse las políticas respectivas a todo el personal.
		A.11.2.2	Servicios de suministro	Los servicios básicos, principalmente el eléctrico telefónico y de internet debe estar adecuado a las necesidades del SGSI
		A.11.2.3	Seguridad del cableado	El cableado eléctrico debe estar separado del cableado de datos y en buen estado, además de que deben limitarse las amenazas asociadas a su destrucción voluntario o intencional por parte de terceros.
		A.11.2.4	Mantenimiento de equipos	Solamente el personal técnico autorizado es quien realizara el mantenimiento de los equipos
		A.11.2.5	Remoción de activos	Los activos retirados de servicio deben ser documentados
		A.11.2.7	Disposición o reutilización segura de equipos	Los dispositivos retirados deben ser dispuesto de manera segura y que se garantice que de los mismos no se podrá extraer información de relevancia para la institución, este proceso debe ser documentado.
		A.11.2.9	Políticas de escritorio limpio y pantalla limpia	Toda información documental física o electrónica debe mantenerse almacenada de forma segura fuera de la vista o alcance de personas no autorizadas
A.12 (Seguridad de las operaciones)	A.12.1 (Procedimientos operacionales y	A.12.1.1	Procedimientos de operativos documentados	deben documentarse todos los procedimientos asociados a la SI de cada activo.
		A.12.1.2	Gestión de Cambios	El encargado del SGSI debe verificar que cada cambio realizado en los activos no afecte la integridad del SGSI
		A.12.1.3	Gestión de Capacidad	La adquisición de equipos nuevos, debe ser planificada y supervisada por el encargado del SGSI y esta debe obedecer solo a necesidades existentes o proyecciones reales de uso
	A.12.2 (Protección contra códigos	A.12.2.1	Controles contra códigos maliciosos	Debe adiestrarse al personal sobre los peligros asociados a los softwares maliciosos a los que podrían estar expuestos los activos de la información. Se aplicara la documentación generada sobre uso de softwares y la verificación periódica por medio de antivirus actualizados y legales.
	A.12.3 (Respaldo)	A.12.3.1	Respaldo de la información	Se deben realizar de manera periódica respaldos de la información de todos los dispositivos, estas serán almacenadas en medios físicos (DVD), en servidores físicos y en la nube. Todos los procedimientos deben estar documentados.

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
	A.12.4 (Copias de respaldo)	A.12.4.1	Registro de eventos	Debe considerarse la revisión periódica, sin menoscabo de que en las auditorias esto ocurra, los registros de eventualidades que estén asociados con la SI, esto para tomar los correctivos pertinentes.
		A.12.4.2	Protección de información de registro	Se deben implementar controles de seguridad que aseguren la protección de la información de los registros generados en la institución.
		A.12.4.3	Registros del administrado y del operador	
		A.12.4.4	Sincronización de reloj	Todos los dispositivos informáticos deben poseer una misma referencia de tiempo y esta debe estar sincronizada en cada elemento
	A.12.5 (Control de *software*	A.12.5.1	Instalación de *software* en sistemas operacionales	Los *softwares que se instalen, deben* cumplir con las políticas de SI, y solo debe ser realizado este procedimiento por el personal autorizado para tal asunto.
	A.12.6 (Gestión de la vulnerabilidad	A.12.6.1	Gestión de las vulnerabilidades técnicas	Debe implementarse siempre que sea necesario la metodología MAGERIT para el análisis y gestión de riesgois y vulnerabilidades.
		A.12.6.2	Restricciones sobre la instalación de *software*	La instalación de *software* es realizada sólo por el personal autorizado y con *software* probado y licenciado. El procedimiento de instalación es documentado.
	A.12.7 (Consideraciones sobre auditorías de sistemas de	A.12.7.1	Controles de auditorías de sistemas de información	Se deben establecer y difundir las fechas de las auditorías internas para los sistemas de información. El procedimiento es documentado.
A.13 (Seguridad de las comunicaciones)	A.13.1 (Gestión de seguridad de la red Objetivo:	A.13.1.1	Controles de redes	Se deben implementar una Infraestructura de Llave Pública (PKI) fuertemente cifrada con la cual se asegure la confidencialidad e integridad de la información que se transmite a través de las redes.
		A.13.1.2	Seguridad de los servicios de red	El acceso a la red de los proveedores de servicio de red debe monitorearse y controlarse por los medios que sea posible.

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
		A.13.1.3	Segregación de redes	Las redes deben segmentarse con acceso restringido y protegido a las mismas, estando en estas separadas el uso de estudiantes y profesores con respecto a la del personal administrativo.
	A.13.2 (Transferencia de información)	A.13.2.1	Políticas y procedimientos de transferencia de información	Las políticas y procedimientos para la transferencia de la información deben mantenerse documentados.
		A.13.2.2	Acuerdos sobre la transferencia de información	Deben crearse e implementarse normas estrictas para el manejo y transferencia de la información.
		A.13.2.3	Mensajería electrónica	Solo deben emplearse los correos institucionales para transmitir información a distintos niveles internos o externos a la unidad educativa.
		A.13.2.4	Acuerdos de confidencialidad o no divulgación	En los documentos contractuales debe especificarse y resaltarse la necesidad de cumplimiento obligatorio de las políticas de SI implementadas con el SGSI
A.14 (Adquisición, desarrollo y mantenimiento de sistemas)	A.14.1 (Requisitos de seguridad de los sistemas de	A.14.1.1	Análisis y especificación de requisitos de SI	Deben establecerse y documentarse los estándares que deben poseer los equipos que se adquieran para que se integren adecuadamente y sin demoras al SGSI.
		A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	Queda prohibido el uso de redes sociales por cualquier persona desde la institución con la única excepción de los encargados de manejar las redes a las que pertenece la unidad educativa.
		A.14.1.3	Protección de transacciones de los servicios de aplicaciones	
	A.14.2 (Seguridad en los procesos de desarrollo y soporte)	A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	De ser necesario cambies en la plataforma de los sistemas, las aplicaciones deben ser aprobadas por el personal especializado y se debe asegurar que no sean una amenaza para las políticas de seguridad existentes.
		A.14.2.7	Desarrollo contratado externamente	De necesitarse softwares especializados, como por ejemplo los administrativos, debe asegurarse junto con el desarrollador que este se adapte a las políticas de seguridad del SGSI
		A.14.2.8	Pruebas de seguridad de sistemas	Se deben realizar pruebas periódicas programadas sobre la seguridad de los sistemas informáticos, esta actividad debe ser realizada por personal competente y capacitado para tal fin y todo el proceso debe ser documentado.
		A.14.2.9	Pruebas de aceptación de sistemas	
	A.14.3 (Datos de prueba)	A.14.3.1	Protección de datos de prueba	
A.15 (Relaciones	A.15.1 (SI en las	A.15.1.1	Política de SI para las relaciones con los proveedores	Deben establecerse y difundirse las políticas de seguridad asociadas a los proveedores externos

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
		A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	
		A.15.1.3	Cadena de suministro de tecnología de información y comunicación	
	A.15.2 (Gestión de la prestación de	A.15.2.1	Monitoreo y revisión de servicios de los proveedores	
		A.15.2.2	Gestión de cambios en los servicios de los proveedores	
A.16 (Gestión de incidentes de SI)	A.16.1 (Gestión de incidentes de SI y mejoras)	A.16.1.1	Responsabilidades y procedimientos	Se debe mantener documentado y actualizado el plan de continuidad de negocios así como definidos los responsables y procesos asociados con el sistema de gestión de la información
		A.16.1.2	Reporte de eventos de SI	Los funcionarios están alertados de los eventos e incidentes correspondientes relativos a la SI. Y los mismos han de estar debidamente documentados con las indicaciones de los correctivos a asumir.
		A.16.1.3	Reporte de debilidades de SI	Deben generarse y difundirse formatos de reportes adecuados para notificar los eventos de seguridad observados
		A.16.1.4	Evaluación y decisión sobre eventos de SI	
		A.16.1.5	Respuesta a incidentes de SI	Deben estar documentadas y actualizadas las posibles respuestas a los incidentes de seguridad.
		A.16.1.6	Aprendizaje obtenido de los incidentes de SI	
		A.16.1.7	Recolección de evidencia	Existen formatos y documentos para recolectar la evidencia de los elementos de riesgos o incidentes de seguridad integrados dentro de los informes de cada reporte.
A.17 (Aspectos de SI de la gestión de la continuidad del negocio)	A.17.1 (Continuidad de SI)	A.17.1.1	Planificación de la continuidad de la SI	Los procesos de revisión, implementación y verificación de la SI deben estar documentados y deben ser entendibles para todo el personal implicado en la ejecución de los mismos
		A.17.1.2	Implementación de la continuidad de la SI	
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la SI	
	A.17.2 (Redundancias)	A.17.2.1	Instalaciones de procesamiento de la información	Debe aclararse en el plan de continuidad de negocios los recursos necesarios para la gestión de la información en las eventualidades en las que este deba implementarse
A.18 (Cumplimiento	A.18.1 (Cumplimiento	A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Los requisitos contractuales y legales se encuentran actualizados y en regla con las disposiciones legales vigentes.

Anexo	Sub punto	Apartado	Control ISO Aplicable	Implementación
		A.18.1.3	Protección de registros	Los registros están protegidos físicamente contra alteración, modificación, pérdida y acceso de usuarios no autorizados.
		A.18.1.4	Privacidad y protección de información de datos personales	Los datos personales son almacenados y protegidos de acuerdo a las conformidades de la ley y regulaciones.
	A.18.2 (Revisiones de SI)	A.18.2.1	Revisión independiente de la SI	Debe documentarse y aprobarse los procesos de auditoria externa
		A.18.2.2	Cumplimiento de políticas y normas de seguridad	
		A.18.2.3	Revisión del cumplimiento técnico	

Fuente: ISO (2014). Diagramado por el Autor.

4.15. Plan de tratamiento de riesgos.

4.15.1. Propósito.

La finalidad de plan de tratamiento de los riesgos de la SI, tiene por finalidad el establecer de manera clara y precisa los controles más idóneos para hacer frente a las eventualidades observadas, para esto, se emplea como base procedimental lo establecido para tal fin en la metodología MAGERIT (CSAE, 2012a).

4.15.2. Tratamiento de riesgos

Los riesgos son tratados en base a lo dispuesto en la metodología MAGERIT, para lo cual, y con el objetivo de facilitar y estandarizar su interpretación, se emplean las definiciones de acciones incluidas en dicha metodología (Anexo 8).

La aplicación de los correctivos o salvaguardas que se muestran a continuación deben ser priorizados por parte del órgano institucional encargado de la administración del SGSI, y debe abordarse en primera instancia los riesgos más graves.

4.15.3. Aplicabilidad de los controles de seguridad

La aplicación de los controles que se muestran a continuación, están sustentados en las recomendaciones de la normativa ISO 27001 (2014) y la MAGERIT (2012a), la prioridad operativa de los mismos, es la de establecer las bases para que la instauración del SGSI sea adecuada, por lo cual, se busca con estos, eliminar en la medida de lo posible los riesgos y vulnerabilidades detectadas para que el sistema de gestión tal como lo indica la norma sea considerado como operativo (***Tabla 14***).

Tabla 14. ***Aplicabilidad de controles en los activos "Datos/Información" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT***

Código del activo	AMENAZA	Riesgo	Tratamiento según MAGERIT (Anexo 8).	SALVAGUARDA (Ver libro 2 de MAGERIT, paginas 53-56)
D_BCK	E*, A*	A	DC	D: Protección de la Información D.A: Copias de seguridad de los datos D.C: Cifrado de la información
D_CNT	E*, A*	MA	DC	D.C: Cifrado de la información D.DS: Uso de firmas electrónicas D.I: Aseguramiento de la integridad
D_HAC	E*, A*	MA	DC	D.C: Cifrado de la información D.DS: Uso de firmas electrónicas D.I: Aseguramiento de la integridad
D_HLB	E*, A*	MA	DC	D.C: Cifrado de la información D.DS: Uso de firmas electrónicas D.I: Aseguramiento de la integridad
D_PUB	E*, A*	MB	DC	D.A: Copias de Seguridad de los datos
D_LOG	E*, A*	A	DC	D: Protección de la Información D.C: Cifrado de la información
D_SRC	E*, A*	MA	DC	D: Protección de la Información D.C: Cifrado de la información
S_MAI	E*, A*	A	DC	S.email: Protección del correo electrónico S.www: Protección de servicios y aplicaciones web
S_GID	E*, A*	MA	DC	S.A: Aseguramiento de la disponibilidad S.dir: Protección del directorio S.SC: Se aplican perfiles de seguridad
S_INT	E*, A*	MA	DC	S.A: Aseguramiento de la disponibilidad S.dns: Protección del servidor de nombres de dominio (DNS)
S_WW W	E*, A*	A	DC	S.A: Aseguramiento de la disponibilidad S.www: Protección de servicios y aplicaciones web
SW_ST D	I*, E*, A*	MA	DC	SW: Protección de las Aplicaciones Informáticas SW.A: Copias de seguridad (backup) SW.SC: Se aplican perfiles de seguridad
SW_MA I	I*, E*, A*	MA	DC	SW: Protección de las Aplicaciones Informáticas SW.SC: Se aplican perfiles de seguridad
SW_DB S	I*, E*, A*	MA	DC	SW: Protección de las Aplicaciones Informáticas SW.A: Copias de seguridad (backup) SW.CM: Cambios (actualizaciones y mantenimiento)

				SW.SC: Se aplican perfiles de seguridad
SW_OF M	I*, E*, A*	B	DC	SW: Protección de las Aplicaciones Informáticas SW.A: Copias de seguridad (backup) SW.SC: Se aplican perfiles de seguridad
SW_AV S	I*, E*, A*	M	DC	SW: Protección de las Aplicaciones Informáticas SW.SC: Se aplican perfiles de seguridad
SW_OP S	I*, E*, A*	M	DC	SW: Protección de las Aplicaciones Informáticas SW.A: Copias de seguridad (backup) SW.SC: Se aplican perfiles de seguridad
HW_BC K	I*, E*, A*	MA	DC	HW: Protección de los Equipos Informáticos
HW_FR W	I*, E*, A*	MA	DC	HW: Protección de los Equipos Informáticos HW.A: Aseguramiento de la disponibilidad HW.SC: Se aplican perfiles de seguridad
HW_HO S	I*, E*, A*	MA	DC	HW: Protección de los Equipos Informáticos HW.A: Aseguramiento de la disponibilidad HW.SC: Se aplican perfiles de seguridad
HW_PC M	I*, E*, A*	B	DC	HW: Protección de los Equipos Informáticos
HW_PC P	I*, E*, A*	B	DC	HW: Protección de los Equipos Informáticos
HW_PR T	I*, E*, A*	MB	AS	HW: Protección de los Equipos Informáticos HW.print: Reproducción de documentos
HW_RO U	I*, E*, A*	A	DC	HW: Protección de los Equipos Informáticos HW.A: Aseguramiento de la disponibilidad HW.SC: Se aplican perfiles de seguridad
HW_SC N	I*, E*, A*	MB	AS	HW: Protección de los Equipos Informáticos
HW_SW H	I*, E*, A*	A	DC	HW: Protección de los Equipos Informáticos HW.A: Aseguramiento de la disponibilidad HW.SC: Se aplican perfiles de seguridad
HW_WA P	I*, E*, A*	B	DC	HW: Protección de los Equipos Informáticos HW.A: Aseguramiento de la disponibilidad
COM_IN T	E*, A*	MA	DC	COM: Protección de las Comunicaciones COM.A: Aseguramiento de la disponibilidad COM.C: Protección criptográfica de la confidencialidad de los datos intercambiados
COM_L AN	E*, A*	MA	DC	COM: Protección de las Comunicaciones COM.A Aseguramiento de la disponibilidad COM.C: Protección criptográfica de la confidencialidad de los datos intercambiados
COM_W IF	E*, A*	M	DC	COM: Protección de las Comunicaciones

				COM.A: Aseguramiento de la disponibilidad COM.C: Protección criptográfica de la confidencialidad de los datos intercambiados COM.wifi: Seguridad Wireless(WiFi)
AUX_F BO	I*, E*, A*	MA	DC	AUX.A: Aseguramiento de la disponibilidad AUX.AC: Climatización AUX.power: Suministro eléctrico
AUX_R CK	I*, E*, A*	A	DC	AUX.A: Aseguramiento de la disponibilidad AUX.AC: Climatización AUX.power: Suministro eléctrico
AUX_P WR	I*, E*, A*	MA	DC	AUX.A: Aseguramiento de la disponibilidad AUX.AC: Climatización AUX.power: Suministro eléctrico
AUX_U PS	I*, E*, A*	A	DC	AUX.A: Aseguramiento de la disponibilidad AUX.AC: Climatización AUX.power: Suministro eléctrico
AUX_WI R	I*, E*, A*	MA	DC	AUX.A: Aseguramiento de la disponibilidad AUX.power: Suministro eléctrico AUX.wires: Protección del cableado
L_SIT	N*, I*, E*, A*	A	AS	L: Protección de las Instalaciones L.A: Aseguramiento de la disponibilidad L.AC: Control de los accesos físicos
P_ADM	E*, A*	A	TT	PS: Gestión del Personal PS.A: Aseguramiento de la disponibilidad PS.AT: Formación y concienciación
P_COM	E*, A*	MA	TT	PS: Gestión del Personal PS.A: Aseguramiento de la disponibilidad PS.AT: Formación y concienciación
P_DBA	E*, A*	MA	TT	PS: Gestión del Personal PS.A: Aseguramiento de la disponibilidad PS.AT: Formación y concienciación
P_DES	E*, A*	M	TT	PS: Gestión del Personal PS.A: Aseguramiento de la disponibilidad PS.AT: Formación y concienciación
Amenazas: [I] De origen industrial; [E] Errores y fallos no intencionados; [A] Ataques intencionados; [N] Desastres naturales. Ri: (Riesgo; A: Alto; MA: Muy Alto; M: Medio; MB: Muy Bajo; B: Bajo); TT: Transferir a Terceros; DC: Definir Controles; AS: Asumir Control				

Fuentes: ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

4.16. Plan de continuidad

4.16.1. Propósito.

Los planes de continuidad de negocios tienen por finalidad garantizar que las instituciones para la cual son creados, ´puedan mantener activas sus actividades a pesar de la ocurrencia de eventos de seguridad ajenos a los diversos stakeholders de la institución, como, por ejemplo, eventos naturales u otro tipo de accidentes.

En este sentido dentro del plan que se propone este plan persigue el mismo objetivo que se plantea, con lo que, se garantiza que tras un incidente la información no se pierda y sea repuesta de manera adecuada y eficiente, con lo que se podría garantizar que al menos con la mínima información posible salvaguardada pueda retomar sus actividades normales.

4.16.2. Objetivos

Los objetivos asociados al plan de continuidad que se plantea son los siguientes:

- Ser una orientación efectiva para la recuperación de las operaciones de la institución tras la ocurrencia de un desastre.
- Asegurar la obtención de los recursos y garantizar la aplicación de política, procesos y procedimientos, para recuperar las actividades de la institución tras la ocurrencia de algún tipo de desastre.
- Definir quiénes son los responsables de la reactivación de las actividades, disminuyendo así las confusiones o desconciertos que pudieran generarse por la acefalia o la descoordinación generada por el respectivo incidente de seguridad.
- Definir de qué forma deben respaldarse o resguardarse los activos de la información en procura de solventar con la mayor premura las situaciones de desastre

4.16.3. Definiciones

Para este apartado se emplearan yodas y cada una de las definiciones adoptadas por el documento normativos de la metodología MAGERIT v3.0 (2012a, págs. 97-105).

4.16.4. Usuarios

Los usuarios a los que está dirigido el plan de continuidad son todos los stakeholders internos y/o externos a los que corresponda por autoridad y competencias, reestablecer las actividades de negocios tras alguna eventualidad.

4.17. Plan de continuidad del negocio

4.17.1. Contenido del plan

En este documento, se definen cuáles son las personas encargadas de la reactivación de las actividades tras la ocurrencia de algún desastre que tenga como consecuencia la paralización temporal de las actividades.

En él se establece los momentos en los cuales se activa o desactivan las actividades de contingencia, y cuáles son los procedimientos y el orden a seguir para su implementación.

Por lo antes expuesto, queda claro que la activación del mencionado plan, solo se realizará en situaciones particulares y tendrá la duración necesaria para solventar las dificultades generadas por la eventualidad que dio origen a su activación.

4.17.2. Roles y responsabilidades

Las personas encargadas de la implementación del plan de continuidad de negocios, tendrá las siguientes asignaciones y responsabilidades que se muestran en la tabla 4.6, mismas que son las estrictamente recomendadas en la Norma ISO 27001:2013 (2013).

Tabla 15. ***Roles y responsabilidades del personal que debe poner en marcha el plan de recuperación o continuidad de negocios.***

ROL	RESPONSABILIDADES
Gerente del BCP	Encargarse de la coordinación general del BCP, tanto a nivel operativo como de logística, haciéndose cargo de las decisiones y los empleados. Desarrollar los métodos y estrategias para la implementación más adecuada del BCP, con el fin de alcanzar los objetivos de seguridad y operatividad en el menor tiempo posible. Garantizar por cualquier vía que los procesos críticos de la institución no se detengan a pesar de la situación que incentivo a la activación del plan, para así, mantener funcionando a la institución
Administrador del BRP	Valorar las situaciones y discutir la prioridad de los gastos necesarios para la restitución de la operatividad Justificar las inversiones adicionales al BRP.
Jefe de recuperación técnica operativa	Trabajar conjuntamente con los otros responsables del BCP para proveer evaluación y requerimientos técnicos para una efectiva recuperación. Diseñar las herramientas de evaluación para determinar el nivel apropiado de los servicios de recuperación. Evaluar la resistencia y las capacidades de recuperación y riesgos inherentes a la infraestructura de TI. Proveer el uso de nuevas tecnologías y procesos para soportar la recuperación de desastres de TI.

Fuente: Desarrollado a partir de las indicaciones de la Norma ISO 27001:2013 (2013). Diagramación por el autor.

4.17.3. Contactos claves

La institución debe crear y establecer de manera publica una lista de contactos que están asociados a las personas, en las que en orden de prioridad pueden irse notificando eventualidades que supongan la posibilidad de la activación del plan de continuidad del negocio, estas, pueden ser las mismas escogidas para ocupar los roles previamente indicados.

4.17.4. Activación y desactivación del plan

Como se ha venido mencionando hasta el momento, el plan de continuidad de los negocios se activará cuando ocurra o sea evidente la ocurrencia de alguna contingencia que se listan a continuación (aunque no limitados a ellos únicamente) se muestran:

- Eventos o desastres que se asocien con la suspensión del servicio prestado por la institución por más de un día (24 horas).

- Cuando se detecten daños en la infraestructura física que puedan causar daños a la vida humana o que la situación en la que se encuentran representen una suspensión de las actividades por un tiempo mayor a 24 horas.
- Cualquier otro evento de naturaleza natural, humana o técnica, que se asocie con la suspensión de los servicios de manera indefinida.

Al momento de la ocurrencia, o de la eminencia de ocurrencia de algún evento que tenga las características antes listadas, se dará notificación del incidente a los que se encuentren en la lista para que de esta manera pongan en marcha el plan de contingencia.

4.17.5. Comunicación

En el caso de contingencia o desastre se empleará en primera instancia la vía de comunicación celular, no obstante, también se puede emplear la vía de correo electrónico, y en última instancia, en la medida de las posibilidades se ubicarán a las personas de la lista en la dirección de vivienda de cada uno. Igualmente, el reporte de la incidencia no se realizará únicamente a los encargados si no que se procederá dar parte a las autoridades competentes.

4.17.6. Sitios físicos y de transporte

En la generación del plan de continuidad de los negocios, debe quedar claro además de los contactos para notificar los incidentes, cuales son los lugares y los medios en los cuales se tiene respaldada la información más importante, establecer el protocolo de acceso a esta, y donde, por motivos de la eventualidad, tendrá lugar la sede de operaciones para la atención de la emergencia.

4.17.7. Orden de recuperación de actividades

En esta sección del documento o del proceso asociado al plan de continuidad de los negocios, se debe indicar el orden de los procesos a seguir para concretar el plan de continuidad.

En primer lugar, se debe:

1. Verificar la activación total de alas comisiones y de los responsables previamente asignados.
2. Se debe identificar si el sitio escogido para la continuidad de las actividades es el más adecuado, esto tomando como criterio la magnitud y duración del evento que motivo la activación el plan.
3. Se deben identificar los recursos y las opciones con los que se cuenta.
4. Se debe identificar los recursos que se pueden recuperar del lugar donde ocurrió el incidente.
5. Se debe recuperar una copia de los respaldos más importantes operativamente.
6. Debe recuperarse o intentar hacerlo, al hardware y los softwares afectados.
7. Debe recuperarse los sistemas informáticos por medio de las copias de seguridad.
8. Se debe documentar cada etapa mencionando y hacer énfasis en las incidencias más complicadas de resolver, además de incluir los pasos que se siguieron para la recuperación, de manera que quede como respaldo para futuras eventualidades.

4.18. Revisión por la Dirección del SGSI

La junta directiva de la unidad educativa, junto con la comisión directiva del SGSI, revisarán de manera anual posterior a haberse completado la implementación del SGSI las oportunidades de mejora del mismo. Para esto, se apoyarán en los resultados de los procesos de auditoria, o los documentos de incidencias reportados a lo largo del año que se evalúa.

En resumen, la información y documentación que se tomara en cuenta para la mencionada revisión son los siguientes

- Resultados de auditorías y revisiones del SGSI.
- Información que pueda provenir de los diversos stakeholders
- Nuevos procesos documentados bibliográficamente que apunten a mejorar la calidad de los sistemas de gestión de la seguridad de la información.
- Estado de la implementación de las acciones correctivas y preventivas que se hayan asumido.

- Resultados de las evaluaciones de vulnerabilidades o amenazas que no se hubieran corregido adecuadamente y que fueran detectados a partir de análisis de riesgos previos.
- Acciones de seguimiento de revisiones previas de la Dirección.
- Cualquier cambio que pueda afectar al SGSI.

4.19. Lineamientos

En esta sección se muestran los lineamientos procedentes de los controles de la Norma ISO 27002:2009, mismos que son seleccionados en función de los resultados de los análisis de riesgos asociados a los sistemas de información de la Institución y interesan como insumo para la creación de la declaración de aplicabilidad; estos lineamientos pueden ser modificados en base a cambios de normativas (Normas ISO, o legislaciones vigentes) y/o cambios dentro de la institución que ameriten un reajuste de lo dispuesto en esta sección.

En este sentido, todos los empleados, estudiantes, representantes y terceros, tienen la obligación de cumplir estas disposiciones, así como, incorporar la seguridad de la información en sus actividades, además de reportar las incidencias que pudieran presentarse.

Tabla 16. ***Lineamientos***

Organización para la SI	**Compromiso con la SI**	**La Institución por medio de sus directivos y de la comisión directiva del DGSI generaran y brindaran el apoyo necesario para implantar y mantener la SI, mediante la destinación de recursos financieros y humano-técnicos requeridos.**
	Divulgación de Información	Solo la junta directiva de la institución es la encargada de generar la autorización de distribución de determinado tipo de datos que sean considerados como restringidos o confidenciales
	Asesoramiento de Especialistas en SI	La Unidad educativa Gedeón, por medio de la directiva general o la del SGSI, podrá requerir y emplear los servicios de expertos en el tema de la SI cuando sea pertinente y necesario.
	Riesgos Significativos para la SI proveniente de actores externos	La Dirección General y del SGSI deberá identificar que tipos de riesgos para la información son generados cuando se requiere de la participación de actores externos en actividades de la institución, y en base a esto, ajustar políticas y controles para los casos particulares
	Requerimientos de Seguridad en las Relaciones con	Antes de facilitar el acceso a información a terceros, la dirección debe sopesar los riesgos y asumir políticas de resguardo adecuadas.

	Clientes o Proveedores	
	Términos y Condiciones para el Acceso de Terceros	Con la finalidad de estandarizar las actividades de terceros asociadas con manejo, comunicación, visualización o distribución de información, los responsables de esta deben decidir qué acciones seguir para garantizar la integridad de la información.
GESTIÓN DE ACTIVOS	Control de Activos	La Directiva de la institución y del SGSI, deben identificar y llevar un control de los activos importantes relacionados con los procesos, servicios y sistemas de información que los soportan.
	Asignación de Activos	Cada empleados es responsable directo de los activos de la información que están a su cargo y este, debe responder por la integridad de los mismos
	Uso de los Activos	La Directiva de la institución y la del SGSI definirán las directrices para el uso de los activos y será divulgada oportunamente a todos los stakeholders
	Clasificación de la Información	La información generada por cada empleado o estudiante, o la que es confiada a estos por cualquier otra persona, y que este relacionada con la institución, será clasificada y tratada por el creador/receptor como Confidencial, Reservada, o de interés general según sea el caso. La Dirección del SGSI establecerá de manera oportuna estas directrices.
	Marcado y Manejo de la Información	La información confidencial deberá señalarse como tal y estará bajo la responsabilidad del propietario de la misma, el cual, debe tomar las precauciones de almacenamiento más pertinente.
SEGURIDAD ASOCIADA AL RECURSO HUMANO	Responsabilidades y Perfiles de Puestos	Cada empleado debe conocer las responsabilidades específicas de su cargo sobre el tema de la SI
	Términos y Condiciones de Contrataciones	Los contratos a empleados, a contratistas y a otros deben incluir las indicaciones de responsabilidades en el tema de la SI.
	Conocimiento sobre la Documentación del SGSI	La dirección del SGSI se encargara de manera periódica, de difundir información referente a la SI y las normativas aplicables por la institución, esto, será una difusión pública y tiene por objeto adiestrar y concientizar sobre el tema
	Capacitación en SI	La difusión debe completarse con entrenamiento periódico específico sobre el tema de SI, para esto la dirección del SGSI ofrecerá a sus empleados de manera oportuna los talleres y cursos relacionados con el tema de SI
	Cambio o Cese de funciones	Las personas con algún tipo de privilegio de acceso y manejo de información deben ser desincorporados de os sistemas de acceso al dejar de trabajar en la institución.
	Revocación de Derechos de Acceso	
SEGURIDAD FISICA Y AMBIENTAL	Seguridad Física	Cada área de la institución donde se almacenen activos de información, deben definir y acondicionar el perímetro de resguardo de los elementos de información.
	Control de Acceso Físico a la Información Confidencial o Reservada	Las áreas donde se genere o resguarde información sensible y/o de interés para la institución debe tener el acceso físico restringido
	Protección contra Amenazas Externas y del Ambiente	Deben incluirse en las áreas donde se encuentran los activos de la información, todos los elementos de protección posible en contra de eventos naturales
	Trabajos en Áreas Seguras	Los empleados de algún área donde se cree o almacene información o activos informáticos y en las que se encuentren momentáneamente terceras personas, deben asumir las actitudes necesarias para salvaguardar a estas

	Servicios de Soporte	Deben instalarse en los centros donde se maneja o crea información de interés, todos los elementos adecuados para el funcionamiento adecuado de los equipos informáticos, o para la protección de los mismos
	Protección de Equipos Informáticos que contengan Información	
	Cables Eléctricos y de Telecomunicaciones	Para efectuar trabajos de instalación y el mantenimiento de infraestructura eléctrica y de telecomunicaciones, los responsables cumplirán las normas y estándares de seguridad vigentes, con el objeto de ser protegido contra la interceptación o daños.
	Mantenimiento Preventivo y Correctivo	La dirección del SGSI canalizara la implementación de un cronograma periódico de mantenimiento preventivos de los equipos informáticos
CONTROL DE ACCESOS	Política de Control de Acceso	Cada empleado controlara el acceso a los elementos de la información, basándose para esto, en los lineamientos de control de acceso emitidos por la DINAFI.
	Registro de Usuarios	En la sala de computación se deben crear tantas sesiones como alumnos utilicen las computadoras, y deberán ser dados de baja en cada periodo académico o cuando se presente alguna renuncia o despido
	Gestión de Privilegios	La asignación y el uso de privilegios deben estar restringidos y controlados de acuerdo a los lineamientos de control de acceso emitidos por el SGSI.
	Gestión de Contraseñas de usuario	La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal de acuerdo a los lineamientos de control de acceso emitidos por la dirección del SGSI.
	Uso y Estructura de las Contraseñas	Las contraseñas son estrictamente personales e intransferibles y es responsabilidad directa del usuario los incidentes de seguridad que puedan ser causados por descuido, divulgación o mala utilización de ésta.
	Computadores Desatendidos	Los usuarios deben activar el protector de pantalla protegido por contraseña, cuando vayan a dejar sus estaciones de trabajo desatendidas
	Uso de los Servicios de Red	El acceso al internet (por cable o wifi), debe ser regulado por medio de la implementación de algún pasword y el mismo debe ser entregado únicamente por el encargado de informática, este pasword debe ser cambiado periódicamente
	Segregación de Redes de Datos	El área administrativa debe poseer un servicio de internet diferente del resto de la institución, es decir, deben crearse al menos una red para el área administrativa
	Uso de los Recursos del Sistema	Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de .las aplicaciones del negocio de acuerdo a los lineamientos de control de acceso emitidos por la dirección del SGSI.
	Software Estándar en Estaciones de Trabajo	Los diversos computadores deberán contar con sistemas operativos y antivirus actualizados.
	Desinstalación de Software.	La instalación o desinstalación software en las equipos de computación debe ser realizado únicamente por el personal informático autorizado
	Computadores Portátiles con Información Reservada o Confidencial	Los usuarios responsables de computadores portátiles que contengan información reservada o confidencial, se apoyarán en las unidades de informática de la Dirección o Dependencia para garantizar que dichos equipos cuenten con medidas de

		seguridad, por ejemplo: contraseña de arranque, usuario y contraseña de sistema operativo.
GESTION DE INCIDENTES	Notificación de los Eventos de Seguridad de la Información	Los empleados, contratistas y usuarios de las aplicaciones del negocio, software en general y servicios de información de la Institución, deben reportar oportunamente los eventos de seguridad de la información

4.20. Mejora continua

Para asegurar una implementación adecuada del ciclo de mejora continua de Deming, la unidad educativa realizara de manera anual, una sesión de revisión de los resultados de las auditorias, mismas que también deben ejecutarse anualmente. En base a esto, se tomarán los correctivos pertinentes y se establecerán estrategias para reforzar o mejorar la seguridad de otras políticas que no se vieran comprometidas en la evaluación.

Todos los resultados de esta evaluación, deben ser documentados y descritos de manera adecuada para poder mantener un registro de las variaciones implementadas. En este caso, la directiva del SGSI se encargará de hacer seguimiento de los acuerdos adoptados en esta materia, y también documentará la implementación de los mismos cuando estos se concreten.

CONCLUSIONES

Mediante la implementación de esta investigación, se logró conocer de qué manera la configuración de trabajo de la unidad educativa, así como las políticas existentes y el estado de los activos informático. Contribuyen a los riesgos de perdida de información vital de la institución.

En este sentido, se determinó que la institución incumple en más del 79,87% de los aspectos de seguridad que pide la norma ISO 27001:2013 como de obligatorio cumplimiento en el anexo A de la mencionada normativa.

De igual manera se determinó que tampoco cumple en 86,1% de los casos con las disposiciones indicados en los apartados 4 al 10 de la norma ISO empleada (27001:2013), en estos puntos, se valora la adecuación de la institución en aspectos como contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejoras, mismos que son determinantes para evitar la pérdida de información por diversas causas dentro de las instituciones.

Por su parte, la evaluación de riesgo mostró que en el 47,05% de los casos el riesgo asociado a los activos es Muy alto, y solo 8,82% se asoció con una situación de riesgo muy baja. Igualmente, si se considera también el riesgo evaluado en diversos aspectos que dieron por resultado una clasificación de riesgo Alta (23,53%), junto con los ya mencionados resultados de riesgo muy alto, tenemos que el riesgo elevado general observado alcanza el 70,58%.

Todo lo anterior permite concluir que la Unidad Educativa sufre la probabilidad alta de incurrir en la pérdida o daño en sus activos informáticos, por lo que es evidente la necesidad de implementar correctivos que disminuyan o eliminen estos riesgos debido a

que afectarían la integridad no solo de la institución y de sus estudiantes, sino que posiblemente las consecuencias sean transferidas a la asociación adventista nacional a la cual pertenecen.

Entre los elementos importantes dentro de un SGSI de lo que carece la Unidad Educativa se encuentra que carecen totalmente de una documentación de cualquier tipo de procesos, no existe una manera controlada ni ordenada de ejecutar las tareas ni mucho menos de verificar o documentar las fallas de seguridad, vulnerabilidades ni riesgos.

Así mismo, los controles para mitigar los accesos sin autorización a los documentos, y equipos informáticos son laxos, y pueden ser violentados de manera consiente sin muchos esfuerzo e incluso sin la posibilidad de que el infractor sea detectado, esta facilidad de vulnerar los activos de la información se expande incluso a nivel informático debido a que no existen normativas que limiten e uso de dispositivos computacionales ajenos a la institución y las redes de usos de los estudiantes están compartidas con las del uso administrativo, además de que estos, se encuentran desactualizados y empleando softwares informáticos sin licencias.

RECOMENDACIONES

Dadas las carencias manifiestas en las evaluaciones preliminares y considerando a su vez la disposición de la directiva a considerar las observaciones emitidas en este estudio, se recomienda que como manera de comenzar a avanzar en la implementación del SGSI, se generen las facilidades para la creación de protocolos y procesos extensos basados en los activos de la información de los cales disponen. La creación de los respectivos protocolos y procesos seria el principal avance en la vía de la implementación del SG

Así mismo, la inexperiencia del personal actual en materia de informática o SI, son las bases que justifican que la unidad educativa tenga dentro de su personal al menos un empleado capacitado en estas áreas, al cual, se le pueda asignar la responsabilidad de la implementación del sistema de gestión, por lo que la recomendación de contratar a un empleado con estas competencias es más que evidente.

Se recomienda también, que se establezca una planificación presupuestaria y de tiempo que abarque la sustitución de los equipos informáticos actuales por otros más modernos y con softwares licenciados, tanto ofimáticos como antivirus.

También se recomienda que, en el asunto correspondiente a las redes de internet, estas sean reestructuradas y se separen las redes de la sección de administración con la de acceso destinados a estudiantes profesores u otros terceros, con lo cual se lograría blindar los activos de la información más importantes de la institución.

Así mismo, se recomienda que indistintamente este o no implementado el sistema de gestión, se comience con un plan de concientización-capacitación dirigido a todos los stakeholders, de manera que la implementación no sea una sorpresa para ninguna de las

partes interesadas y que la respectiva implementación y aplicación del SGSI se realice lo más pronto posible.

La recomendación más importante es precisamente que lo antes posible se comience con la implementación formal del sistema de gestión y que este esté encaminado en lograr la certificación ISO respectiva.

REFERENCIAS BIBLIOGRÁFICAS

Armijos, A. (2018). *Gestión de riesgos informáticos.* Pachuca - México: Queen ediciones.

Bailón, E., & Bermúdez, K. (2015). *Análisis de la seguridad informática y seguridad de la información basado en la Norma ISO 27001 dirigido a empresas.* Guayaquil - Ecuador: Universidad Politécnica Salesiana.

Barrantes, C., & Hugo, J. (2012). *Diseño e implementación de un sistema de seguridad de la información en procesos Tecnológicos.* Lima: USMP.

BBC Mundo. (21 de marzo de 2018). *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. Obtenido de BBC Mundo: https://www.bbc.com/mundo/noticias-43472797

Benavides, S. (2018). *La seguridad informática.* Dallas - Estados Unidos: Poker ediciones.

Bermúdez, K., & Bailón, E. (2015). *Análisis en seguridad informática y seguridad de la información, Basado en la norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigidoi a una empresa de servicios financieros.* Guayaquil: UPS- Guayaquil.

Berumen, S., & Arriaza, K. (2008). *Evolución y desarrollo de las TIC en la economía del conocimiento.* Madrid, España: Ecobook Editorial de Economista.

Bonilla, M. (2018). *Diseño de un sistema de gestión de seguridad de información bajo la ISO 27000 para la Unidad Educativa particular Séneca.* Quito - Ecuador: Universidad Tecnológica Israel.

Brito, G. (2017). *Los Sistemas de Gestión de Seguridad de Información en procesos de control para instituciones gubernamentales ecuatorianas.* Quito - Ecuador: USFQ publicaciones.

Campo, N. (2013). *Segurança da Informação.* Cuiabá: UFMT.

Cárdenas, L., Martínez, H., & Becerra, L. (2016). Gestión de seguridad de la información: revisión bibliográfica. *El profesional de la información, 25*(6), 931-948.

Castro, A., & Jácome, V. (2017). *Seguridad informática y de control empresarial.* Atlanta - Estados Unidos: Micro ediciones.

Chamorro, V. (2013). *Plan de seguridad de la informacion basado en el estandar ISO 13335 aplicado a un caso de estudio.* Quito: EPN.

COBIT. (2019). *Manual de uso y funcionamiento de COBIT.* Houston - Estados Unidos: COBIT publicaciones.

Cohard, P. (2019). Information Systems Security: Challenges, Vulnerabilities and Tools . En G. N'Goala, V. Pez-Pérard, & I. Prim-Allaz, *Augmented Customer Strategy: CRM in the Digital Age* (págs. 257-270). John Wiley & Sons, Inc.

Crespo, J. (2018). *Indicadores de desarrollo económico en Latinoamérica.* Lima - Perú: Federer ediciones.

CSAE. (2012a). *MAGERIT Libro I - Método – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

CSAE. (2012b). *MAGERIT – versión 3.0. Libro II. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Catálogo de Elementos.* Madrid: CSAE.

CSAE. (2012c). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas.* Madrid: CSAE.

CTIC. (2017). *ANEXO B. Guía Para la Metodología de Gestión de Riesgos.*

Datasec. (2018). *Indicadores de certificados Normas ISO 27001.* Bogotá - Colombia: Datasec publicaciones.

Encalada, D. (2017). *La gestión de riesgos informáticos en las instituciones privadas.* Bogotá - Colombia: Power Siux ediciones.

Fonseca, D. (2017). *Riesgos informáticos.* México D.F. - México: Atenea ediciones informáticas.

Galarza, J. (2018). *Evaluación y control de sistemas de riesgo.* México D.F. - México: Fox ediciones científicas.

Ghazouani, M., Faris, S., Medromi, H., & Sayouti, A. (2014). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications, 103*(8), 36-42.

Gil, D., & Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, *22*(2), 193-197.

Guamán, J. (2015). *Diseño de un sistema de gestión de seguridad de la información para instituciones militares.* Quito - Ecuador: Escuela Politécnica Nacional.

Guamán, J. (2015). *Diseño de un sistemas de gestión de seguridad de la Información para instituciones militares.* Quito: EPN.

Guevara, R. (2017). *Sistema de gestión de seguridad de la información basada en la Norma ISO 27001 para el departamento de tecnologías de la información y comunicación de las Unidades Educativas de Quito.* Ambato - Ecuador: Universidad Técnica de Ambato.

Hoepers, C., & Steding-Jessen, K. (12 de agosto de 2014). *Fundamentos de Segurança da Informação* . Recuperado el junio 08 de 2019, de Web del El Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil (CERT.br): https://www.cert.br/docs/palestras/certbr-egi2014.pdf

Hunter Control Systems. (2019). *Protocolos de seguridad*. Houston - Estados Unidos: HCS ediciones.

Information Technology Infrastructure Library. (2019). *Funcionamiento de ITIL*. Houston - Estados Unidos: ITIL publicaciones.

ISO. (2005). *ISO / IEC 17799: 2005 (Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información).* ISO.

ISO. (2013). *Code of practice for information security controls.* Standard, International Organization for Standardization.

ISO. (2013). *ISO 27001*. Ginebra - Suiza: ISO publicaciones internacionales.

ISO. (2013). *Normativa ISO 27000.* Ginebra - Suiza: ISO publicaciones internacionales.

ISO. (2014). *NTP-ISO/IEC 27001:2014. (EQV. ISO/IEC 27001:2013+ISO/IEC 27001:2013/COR 1 Information technology -- Security techniques --Information security management systems – Requirements).* Lima: NTP.

ISO. (2016). *Information security management systems - Overview and vocabulary.* Standard, International Organization for Standardization.

ISO. (2017). *ISO Survey*. Recuperado el 8 de Junio de 2019, de Web de ISO: https://www.iso.org/the-iso-survey.html

ISO. (2018). *ISO/IEC 27000:2018.* Geneva: ISO.

ISO. (s.f). *ISO/IEC 27000 family - Information security management systems*. Recuperado el 8 de Junio de 2019, de Web de ISO: https://www.iso.org/isoiec-27001-information-security.html

ISOTools. (30 de Marzo de 2015). *ISO 27001: Los activos de información*. Recuperado el 2 de noviembre de 2018, de Blow de SGSI, de ISOTools: https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

ISOTools Excellence. (23 de febrero de 2017). *¿Cómo realizar un inventario de activos de información?* Recuperado el 08 de junio de 2019, de Web de SGSI por ISOTools Excellence: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

Iza, A. (2018). *Automatización del proceso de gestión académica de pre - básica del Instituto Educativo privado Children Genios y Noruega escuela.* Quito - Ecuador: Universidad Tecnológica Israel.

Jiménez, M. (2017). *Administración del sistema de gestión de seguridad de la información de la Secretaría Nacional de Comunicación enfocado a la infraestructura tecnológica.* Quito: Universidad Del Pacífico.

Joya, J., & Sacristán, C. (2017). *Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos para la Empresa Javesalud I.P.S.* Bogotá: Universidad Católica De Colombia. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/15405/1/Proyecto%20Final%20Especializacion%20Seguridad%20de%20la%20Informacion.pdf

Kopertti, R. (2018). *Evaluación de riesgos informáticos.* Bogotá - Colombia: Premier ediciones.

Marciano, J., & Marques, M. (2006). O enfoque social da segurança da informação. *Ci. Inf., Brasília, 35*(3), 89-98.

Marques, G. (2018). *Diagnóstico de gestão da segurança da informação em empresas nacionais do setor financeiro.* Porto Alegre: Universidade Federal do Rio Grande do Sul.

Martin, K., Borah, A., & Palmatier, R. (2017). Data privacy: effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58.

Mier, V. (2017). *Vulnerabilidades en los sistemas informáticos y en bases de datos empresariales.* Caracas - Venezuela: Ecos ediciones académicas.

Minerva, S. (2017). *Estrategias de uso informativo en sistemas empresariales.* Valencia - España: Westeros ediciones.

Ministerio de Educación ecuatoriano. (2019). *Información y manejo institucional.* Quito - Ecuador: Ministerio de Educación ecuatoriano publicaciones.

Ortiz, A. (2017). *Sistemas de control y protección informática para unidades educativas del milenio, caso Quito 2017.* Quito - Ecuador: PUCE publicaciones.

Ortiz, V. (2017). *La seguridad informática.* Madrid - España: Palenque ediciones.

Palacios, Á. (2018). *Auditoría a la seguridad informática en la Dirección Distrital 02D03 Chimbo - San Miguel - Educación durante el período enero 2016 - octubre 2017, utilizando la norma internacional COBIT.* Quito - Ecuador: Universidad Tecnológica Israel.

Pedrosa, X. (2018). *Elementos de la seguridad informática.* México D.F. - México : Poleer ediciones.

Restrepo, C. (2018). *Manejo profesional de los riesgos informáticos.* Managua - Nicaragua: Fortune ediciones.

Ríos, A. (2018). *Implementación de sistemas de seguridad informática.* Dallas - Estados Unidos: Hill ediciones investigativas.

Sampieri, R., Fernández, C., & Baptista, M. (2014). *Metodología de la Investigación* (Sexta ed.). México: McGRAW-HILL.

Sanchez, A. (19 de Mayo de 2011). *Cobit*. Recuperado el 08 de junio de 2019, de Blog de Andrés Felipe Sánchez Diseñador Visual Especialista en Dispositivos Móviles: http://andresvisualdesign.blogspot.com/2011/05/cobit.html

SENPLANDES. (2013). *Esquema Gubernamental de seguridad De La Informacion EGSI. Acuerdo Ministerial 166.* Recuperado el 08 de junio de 2019, de https://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%c3%83%c2%b3n.pdf

Siponen, M., & Willison, R. (2009). nformation security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270.

Tersek, Y. (2008). *Sistema de gestión de seguridad de la información para un sistema de información (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO- Puerto Ordaz).* Barquisimeto: Universidad Centroccidental "Lisandro Alvarado".

Unidad Educativa Adventista Gedeón. (2019). *Unidad Educativa Adventista Gedeón*. Recuperado el 08 de Junio de 2019, de Unidad Educativa Adventista Gedeón: http://ueag.educacionadventista.com/

Vallejo, A. (2018). *Propuesta de Sistema de Gestión de Seguridad de la Información para el centro de datos de la empresa Leterago del Ecuador S.A.* Quito - Ecuador: Universidad Tecnológica Israel.

Valverde, F. (2017). *Sistemas de seguridad informáticos.* México D.F. - México: Bermetti ediciones.

Varela, C. (2017). *El manejo de la seguridad informática en las empresas.* Bogotá - Colombia: Galeón ediciones educativas.

Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. *Proceedings of SAICSIT*, (págs. 95–103).

Wang, P., & Ratchford, M. (2018). Integrated Methodology for InformationSecurity Risk Assessment. En *Information Technology – New Generations, Advances in Intelligent Systems and Computing* (págs. 147-150). Springer International Publishing. doi:DOI 10.1007/978-3-319-54978-1_20

WTW. (12 de Diciembre de 2018). *Riesgo Cibernético*. Recuperado el 8 de junio de 2019, de WTW: https://www.willistowerswatson.com/es-MX/Insights/2018/12/riesgo-cibernetico-mexico-2018

Zambrano, M. (2018). *parámetros de seguridad informática.* Barcelona - España: Lyon gold ediciones digitales.

ANEXOS

Anexo 1: Categorías de las amenazas según el método MAGERIT

Categorización de las Amenazas según la metodología MAGERIT

Tipo de Amenaza	Nomenclatura	Definición
Desastres Naturales	[N]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	[I]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Esta amenaza puede darse de forma accidental o deliberada.
Errores y Fallos No Intencionados	[E]	Fallos no intencionales causados por las personas.
Ataques Intencionados	[A]	Fallos deliberados causados por las personas.

Fuente: CSAE: (2012b). Diagramado por el Autor.

Anexo 2: Tabulación de valor de las amenazas según el método MAGERIT

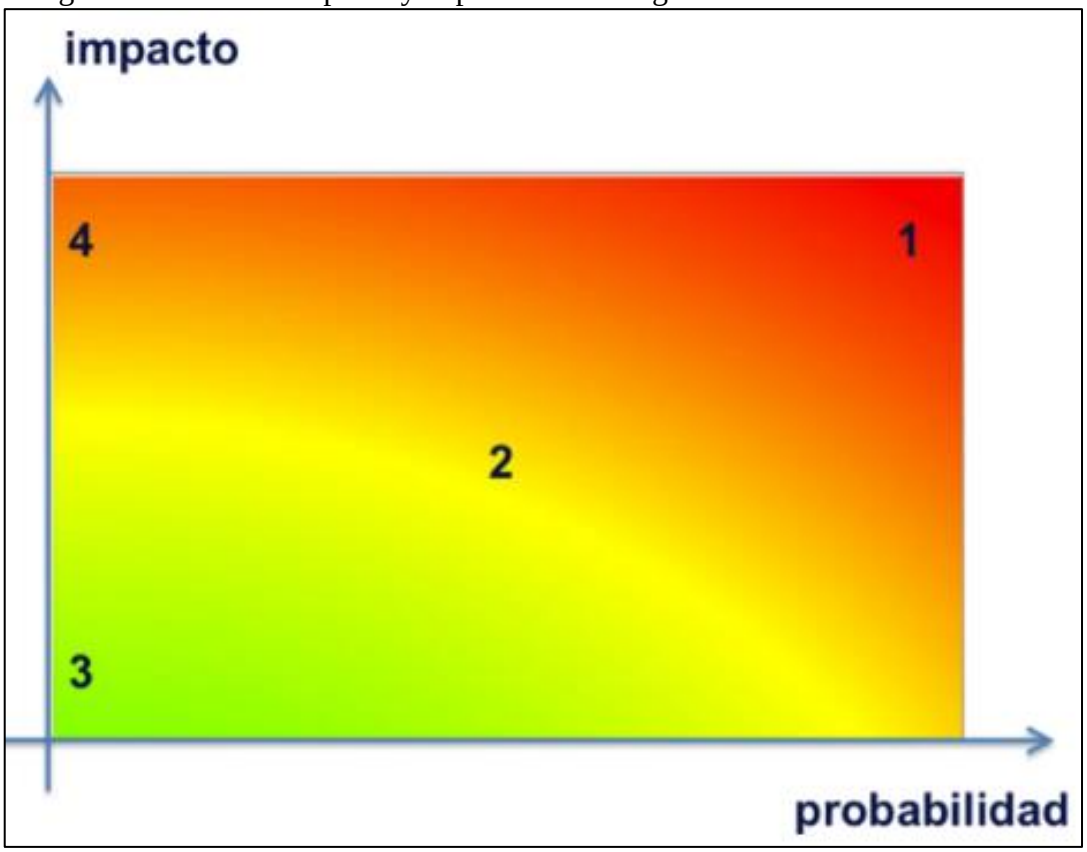
Valoración de las Amenazas según la metodología MAGERIT

Probabilidad o Frecuencia	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: CSAE: (2012a, pág. 28). Diagramado por el Autor.

Anexo 3: Tabulación de riesgos según el método MAGERIT

Riesgo en función del impacto y la probabilidad según el método



MAGERIT. Fuente: CSAE: (2012a, pág. 30).

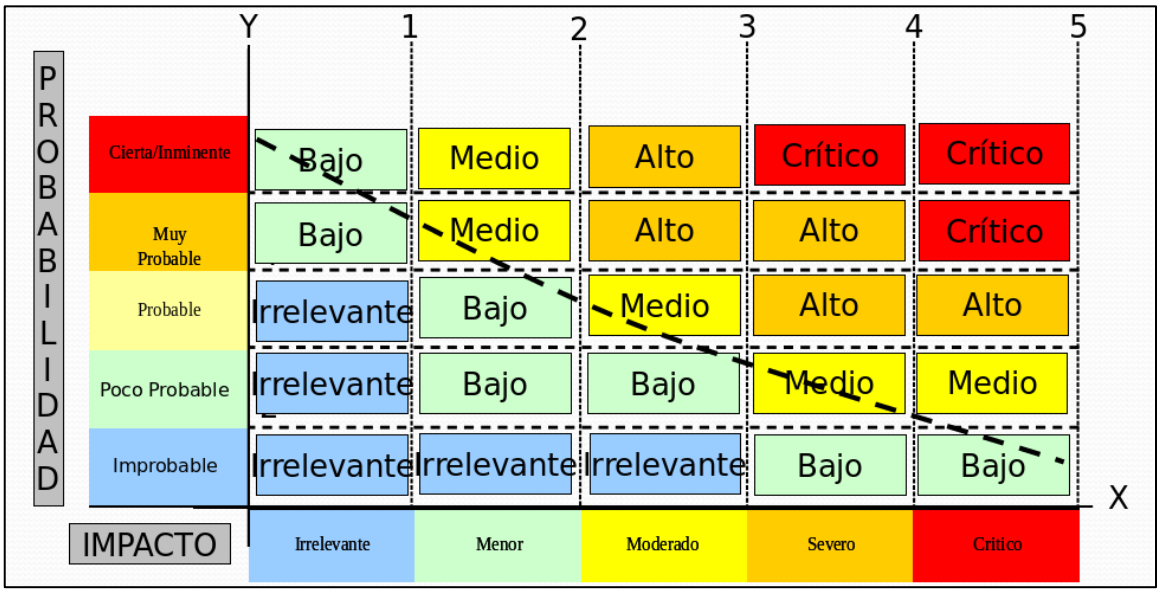
Anexo 4: Tipos de Salvaguardas definidos en el método MAGERIT

Tipos de Salvaguardas definidos en el método MAGERIT

Control	Nomenclatura
Protecciones generales	H
Protección de los datos / información	D
Protección de las claves criptográficas	K
Protección de los servicios	S
Protección de las aplicaciones (*software*)	SW
Protección de los equipos (*hardware*)	HW
Protección de las comunicaciones	COM
Protección en los puntos de interconexión con otros sistemas	IP
Protección de los soportes de información	MP
Protección de los elementos auxiliares	AUX
Seguridad física – Protección de las instalaciones	L
Protecciones relativas al personal	PS
Protecciones de tipo organizativo	G
Continuidad de operaciones	BC
Externalización	E
Adquisición y desarrollo	NEW

Fuente: CSAE (2012b, págs. 53-57). Diagramado por el Autor.

Anexo 5: Matriz Para Valorar el Riesgo según el método MAGERIT



Fuente: CTIC (2017, pág. 15).

Anexo 6: Codificación de los activos informáticos según el método MAGERIT

2.3. [D] Datos / Información

Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

[D] Datos / Información
[files] ficheros [backup] copias de respaldo [conf] datos de configuración (1) [int] datos de gestión interna [password] credenciales (ej. contraseñas) [auth] datos de validación de credenciales [acl] datos de control de acceso [log] registro de actividad (2) [source] código fuente [exe] código ejecutable [test] datos de prueba
(1) Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información. (2) Los registros de actividad sustancian los requisitos de trazabilidad.

2.4. [K] Claves criptográficas

Las criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

[keys] Claves criptográficas
[info] protección de la información [encrypt] claves de cifra [shared_secret] secreto compartido (clave simétrica) (1) [public_encryption] clave pública de cifra (2) [public_decryption] clave privada de descifrado (2) [sign] claves de firma [shared_secret] secreto compartido (clave simétrica) [public_signature] clave privada de firma (2) [public_verification] clave pública de verificación de firma (2) [com] protección de las comunicaciones [channel] claves de cifrado del canal [authentication] claves de autenticación [verification] claves de verificación de autenticación [disk] cifrado de soportes de información [encrypt] claves de cifra [x509] certificados de clave pública
(1) Por ejemplo, DES, 3-DES, AES, etc. (2) Por ejemplo, RSA, Diffie-Hellman, curvas elípticas, etc.

2.5. [S] Servicios

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

[S] Servicios
[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual) [ext] a usuarios externos (bajo una relación contractual) [int] interno (a usuarios de la propia organización)
[www] world wide web [telnet] acceso remoto a cuenta local [email] correo electrónico [file] almacenamiento de ficheros [ftp] transferencia de ficheros [edi] intercambio electrónico de datos [dir] servicio de directorio (1) [idm] gestión de identidades (2) [ipm] gestión de privilegios [pki] PKI - infraestructura de clave pública (3)
(1) Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado. (2) Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización. (3) Servicios asociados a sistemas de criptografía de clave pública, incluyendo especialmente la gestión de certificados.

2.6. [SW] Software - Aplicaciones informáticas

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

No preocupa en este apartado el denominado "código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

[SW] Aplicaciones (software)
[prp] desarrollo propio (in house) [sub] desarrollo a medida (subcontratado) [std] estándar (off the shelf) [browser] navegador web [www] servidor de presentación [app] servidor de aplicaciones [email_client] cliente de correo electrónico [email_server] servidor de correo electrónico [file] servidor de ficheros [dbms] sistema de gestión de bases de datos [tm] monitor transaccional [office] ofimática [av] anti virus [os] sistema operativo [hypervisor] gestor de máquinas virtuales [ts] servidor de terminales [backup] sistema de backup

2.7. [HW] Equipamiento informático (hardware)

Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

[HW] Equipos informáticos (hardware)

[host] grandes equipos (1)
[mid] equipos medios (2)
[pc] informática personal (3)
[mobile] informática móvil (4)
[pda] agendas electrónicas
[vhost] equipo virtual
[backup] equipamiento de respaldo (5)
[peripheral] periféricos
  [print] medios de impresión (6)
  [scan] escáneres
  [crypto] dispositivos criptográficos
[bp] dispositivo de frontera (7)
[network] soporte de la red (8)
  [modem] módems
  [hub] concentradores
  [switch] conmutadores
  [router] encaminadores
  [bridge] pasarelas
  [firewall] cortafuegos
  [wap] punto de acceso inalámbrico
[pabx] centralita telefónica
[ipphone] teléfono IP

(1) Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.

(2) Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.

(3) Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.

(4) Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.

(5) Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.

(6) Dícese de impresoras y servidores de impresión.

(7) Son los equipos que se instalan entre dos zonas de confianza.

(8) Dícese de equipamiento necesario para transmitir datos: routers, módems, etc.

2.8 [COM] Redes de comunicaciones

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

[COM] Redes de comunicaciones
[PSTN] red telefónica [ISDN] rdsi (red digital) [X25] X25 (red de datos) [ADSL] ADSL [pp] punto a punto [radio] comunicaciones radio [wifi] red inalámbrica [mobile] telefonía móvil [sat] por satélite [LAN] red local [MAN] red metropolitana [Internet] Internet

2.9. [Media] Soportes de información

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[Media] Soportes de información
[electronic] electrónicos [disk] discos [vdisk] discos virtuales [san] almacenamiento en red [disquette] disquetes [cd] cederrón (CD-ROM) [usb] memorias USB [dvd] DVD [tape] cinta magnética [mc] tarjetas de memoria [ic] tarjetas inteligentes [non_electronic] no electrónicos [printed] material impreso [tape] cinta de papel [film] microfilm [cards] tarjetas perforadas

2.10. [AUX] Equipamiento auxiliar

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

[AUX] Equipamiento auxiliar
[power] fuentes de alimentación [ups] sistemas de alimentación ininterrumpida [gen] generadores eléctricos [ac] equipos de climatización [cabling] cableado [wire] cable eléctrico [fiber] fibra óptica [robot] robots [tape] ... de cintas [disk] ... de discos [supply] suministros esenciales [destroy] equipos de destrucción de soportes de información [furniture] mobiliario: armarios, etc [safe] cajas fuertes

2.11. [L] Instalaciones

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

[L] Instalaciones
[site] recinto [building] edificio [local] cuarto [mobile] plataformas móviles [car] vehículo terrestre: coche, camión, etc. [plane] vehículo aéreo: avión, etc. [ship] vehículo marítimo: buque, lancha, etc. [shelter] contenedores [channel] canalización [backup] instalaciones de respaldo

2.12. [P] Personal

En este epígrafe aparecen las personas relacionadas con los sistemas de información.

[P] Personal
[ue] usuarios externos [ui] usuarios internos [op] operadores [adm] administradores de sistemas [com] administradores de comunicaciones [dba] administradores de BBDD [sec] administradores de seguridad [des] desarrolladores / programadores [sub] subcontratas [prov] proveedores

Anexo 7: Definición de las acciones a seguir para el tratamiento de los riesgos informáticos según el método MAGERIT

Acción	Descripción
Asumirlos (AS):	La dirección asume el riesgo ya que en este punto se encuentra por debajo de un valor aceptable. Se debe documentar y establecer que la dirección conoce y acepta estos riegos. Estos han de ser controlados y revisados periódicamente de cara a evitar que evolucionen.
Definir controles (DC)	Para reducir mediante la implantación de control que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar lo métodos para iniciar la gestión de estos.
Transferirlos a terceros (TT)	se deben evaluar las opciones y tomar acciones pertinentes en función del valor del activo y del costo de realizar esta transferencia (no solo económico, sino que, el riesgo que conlleva la transferencia del riesgo a un tercero).

Fuente: MAGERIT (CSAE, 2012a). Diagramado por el Autor.

Anexo 8: Resultados de la ejecución del inventario

No	Código	Tipo	Procesador	Velocidad	Capacidad RAM	Capac_ Disco Duro	Equipos ACTIVOS	GARANTIA	SO	Versión	Área de Resguardo	Dueño del Activo	Custodio	Acceso	Responsable	Área Resguardo
01	NA	PCE	INTEL	1,2 GHZ	2 GB	250 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	PADM	PADM	PADM	A-ADMI
02	NA	PCE	INTEL	2,4 GHZ	4 GB	250 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	PADM	PADM	PADM	A-ADMI
03	NA	PCE	INTEL	3 GHZ	4 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	PADM	PADM	PADM	A-ADMI
04	NA	PCE	Intel	3,2 GHZ	6 GB	1000 GB	Si	En Curso	WIN10	OFF PRO 2016	SDIR	RADV	SDIR	SDIR	SDIR	SDIR
05	NA	PCE	Intel	3,2 GHZ	8 GB	1000 GB	Si	En Curso	WIN10	OFF PRO 2016	DIRG	RADV	REC	REC	REC	RECT
06	NA	PCE	AMD	3 GHZ	4 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	PADM	PADM	PADM	A-ADMI
07	NA	Laptop	INTEL	1,2 GHZ	2 GB	250 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
08	NA	Laptop	INTEL	1,2 GHZ	2 GB	250 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
09	NA	Laptop	INTEL	1,2 GHZ	2 GB	250 GB	No	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
10	NA	Laptop	INTEL	1,2 GHZ	2 GB	250 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
11	NA	Laptop	INTEL	1,2 GHZ	2 GB	250 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	DOCECT	DOCECT	DOCECT	A-ADMI
12	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	ADM	UED	DIRAC	DIRAC	DIRAC	DIRACD
13	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
14	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	No	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
15	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
16	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
17	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
18	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	No	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
19	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
20	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
21	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP
22	NA	PCE	Intel	3,2 GHZ	8 GB	500 GB	Si	Concluida	WIN-SEVEN	OFF PRO 2010	SCOMP	UED	DOCECT	STD	DOCENT	SCOMP

Anexo 9: Activos y nivel de vulnerabilidad detectados en la Unidad Educativa Adventista Gedeón

	Descripción del activo	Tipo	Electrónica	Dueño del activo	Acceso	Responsable	AUTENTICACIÓN	INTEGRIDAD	CONFIDENCIALIDAD	Valor
INSTALACIONES	Oficina del área administrativa	TANGIBLE		Unidad Educativa	Empleados y público en general	Administración	Alta	Crítica	Restringida	Alta
	Oficina Rectorado	TANGIBLE		Unidad Educativa	Rector	Rector	Alta	Crítica	Restringida	Alta
	Oficina Vice Rectorado	TANGIBLE		Unidad Educativa	Administrativos y docentes	Vice Rector	Alta	Crítica	Restringida	Alta
	Oficina del Inspector académico	TANGIBLE		Unidad Educativa	Administrativos, docentes, estudiantes y representantes	Inspector Académico	Alta	Crítica	Restringida	Alta
	Aula de computación	TANGIBLE		Unidad Educativa	Docentes y estudiantes	Docente de computación	Baja	Crítica	Restringida	Alta
	Salones de clases	TANGIBLE		Unidad Educativa	Docentes y estudiantes	Docente	Normal	Crítica	Restringida	Normal
HARDWARE	Computadores de mesa o laptops de uso institucional	TANGIBLE	Ordenadores	Unidad Educativa	Personal administrativo y docente	Administración	Normal	Alta	Restringida	Alta
	Rúter principal de la Unidad Educativa	TANGIBLE	Enrutadores	CNT	Administración	Administración	Baja	Alta	Protegida	Normal
	Rúter principal del área de Administración	TANGIBLE	Enrutadores	CNT	Administración	Administración	Normal	Alta	Protegida	Normal
	PA Inalámbricos Wifi	TANGIBLE	Enrutadores	CNT	Administración, docentes y público en general	Administración	Normal	Baja	Restringida	Normal
	Impresoras	TANGIBLE	Impresoras	Unidad Educativa	Administración	Administración.	Baja	Baja	Libre	Baja
	Video Beans	TANGIBLE	Proyectores	Unidad Educativa	Docentes	Administración, Docentes	Baja	Baja	Libre	Baja
	Teléfonos celulares personales y institucionales	TANGIBLE	Celulares	Unidad educativa, empleados, representantes	Según pertenencia	Según pertenencia	Normal	Baja	Restringida	Normal

APLICACIONES/ SOFTWARE	Sistemas Operativos	INTANGIBLE	Ordenadores	Microsoft	Usuarios de los activos	Usuarios de los activos	Alta	Crítica	Confidencial	Alta
	Ofimática	INTANGIBLE	Ordenadores	Microsoft	Usuarios de los activos	Usuarios de los activos	Alta	Alta	Restringida	Alta
DATOS/INFORMACION	Facturas	INTANGIBLE	Ordenadores	Unidad Educativa	Administración	Administración	Crítica	Normal	Restringida	Alta
	Pagos del personal	INTANGIBLE	Archivador/estantes	Administración	Administración	Administración	Crítica	Alta	Protegida	Alta
	Contratos de empleados	INTANGIBLE	Archivador/estantes	Administración	Administración	Administración	Normal	Alta	Restringida	Normal
	Notas Académico	INTANGIBLE	Archivador-Estantes/Computadoras	Administración	Administración	Administración	Crítica	Alta	Confidencial	Alta
	Informes psicológicos y administrativos en general	TANGIBLE	Archivador-Estantes/Computadoras	Administración	Administración	Administración	Normal	Crítica	Protegida	Alta
	Registros de inscripciones	TANGIBLE	Ordenadores	Administración	Administración	Administración	Normal	Alta	Restringida	Alta
REDES /COMUNICACIONES	Internet	INTANGIBLE	Enrutadores	CNT	Administración	Administración	Crítica	Alta	Restringida	Alta
	Red de Área Local	INTANGIBLE	Enrutadores	Unidad Educativa	Administración	Administración	Alta	Normal	Restringida	Normal
	Conexión Wifi	INTANGIBLE	Enrutadores	CNT	Administración	Administración	Normal	Baja	Libre	Baja
PERSONAL	Administrativo	TANGIBLE		Unidad Educativa	Administración	Administración	Crítica	Crítica	Protegida	Alta
	Docente	TANGIBLE		Unidad Educativa	Administración	Administración	Alta	Alta	Protegida	Alta
	Visitantes	TANGIBLE			Administración	Administración	Normal	Baja	Restringida	Normal
	Estudiantes	TANGIBLE			Estudiantes	Institución	Alta	Alta	Protegida	Alta

Tabla diagramada por el Autor.

Anexo 10: Resultado de la evaluación de cumplimiento de los puntos 4 al 10 de la Norma ISO 27001:2013

Requisito		Aspecto a considerar	Cumple	% Cumplimiento
4.1	Contexto de la Organización	Comprende a la organización y su contexto.	Si	50%
4.2		Comprende las necesidades y expectativas y obligaciones de las partes interesadas.	No	
4.3		Está definido del alcance del SGSI.	Si	
4.4		Existencia de un SGSI.	No	
5.1	Liderazgo	Esta establecida una línea de Liderazgo y esta, está Comprometida con la implementación del SGSI.	Si	33.3%
5.2		Existen políticas claras y definidas en cuanto al control y manejo de la información.	No	
5.3		Se conocen los roles, responsabilidades y autoridades organizacionales con respecto al SGSI.	No	
6.1.1	Planificación	Existen acciones generalidades para tratar los riesgos y oportunidades.	No	0%
6.1.2		Existe un método de valoración de los riesgos de la SI.	No	
6.1.3		Existe una forma de identificación de los avances en el tratamiento de los riesgos de la SI.	No	
6.2		Están definidos y documentados los objetivos de la SI, así como los planes para alcanzar dichos objetivos.	No	
7.1	Soporte	Existen recursos o dispersión para asignar estos para la implementación del SGSI.	Si	14,3%
7.2		Esta disponible personal competente que se pueda encargar del SGSI una vez que se implemente.	No	
7.3		Se ha realizado alguna campaña institucional para la difusión de importancias y alcances de un SGSI.	No	
7.4		Se emplean adecuadamente los medios de información institucionales para divulgar lo concerniente al SGSI.	No	
7.5.1		Se posee información sobre los SGSI	No	
7.5.2		Existen documentos de documentación de un SGSI que se pueda actualizar.	No	
7.5.3		Existe controles para los documentos del SGSI	No	
8.1	Operación	Existen controles de los procesos aplicables a los objetivos del SGSI.	No	0%
8.2		Existe una valoración de riesgos previa	No	
8.3		Existe una planificación o metodología asociada a la corrección de los Riegos de SI	No	
9.1	Evaluación del Desempeño	Existen procesos de SI que puedan ser evaluados	No	0%
9.2		Hay algún plan de auditoría Interna	No	
9.3		Existe algún plan de revisión por parte de la dirección del plantel sobre el SGSI	No	
10.1	Mejora	Se tiene un plan para tratar las no Conformidades en los procesos relacionados con el SGSI	No	0%
10.2		Existe un plan de mejora continua	No	
Proporción promedio de (Cumplimiento)/(No cumplimiento)				13,9%/86,1%

Anexo 11: Valoración de los riesgos de los activos informáticos

CODIGO	DESCRIPCION	IMPACTO	Puntuación por DIMENSIÓN DE SEGURIDAD					PROBABILIDAD	AMENAZA	RIESGO
			[D]	[I]	[C]	[A]	[T]			
D_BCK	Copias de Seguridad de los Sistemas de Información	MA	3		2			MB	E*, A*	A
D_CNT	Contratos	MA		2				M	E*, A*	MA
D_HAC	Historial Académico	MA		4	7	4	4	B	E*, A*	MA
D_HLB	Historial Laboral	MA		3	2			B	E*, A*	MA
D_PUB	Publicaciones	B	1					MB	E*, A*	MB
D_LOG	Registros de Actividad	MA	1		2		3	MB	E*, A*	A
S_MAI	Correo Electrónico	A	3		2			M	E*, A*	A
S_GID	Gestión de Identidades	MA	5	2	2		4	M	E*, A*	MA
S_INT	Servicios Internos	MA	3					M	E*, A*	MA
S_WWW	Página web	A	3					M	E*, A*	A
SW_STD	*Software* Estándar	MA	5				1	M	I*, E*, A*	MA
SW_MAI	*Software* para Correo Electrónico	A	7	7	7	7		A	I*, E*, A*	MA
SW_DBS	Gestores de Bases de Datos	MA	1					B	I*, E*, A*	MA
SW_OFM	Ofimática	B			7			M	I*, E*, A*	B
SW_AVS	*Software* de Antivirus	M	5	7				M	I*, E*, A*	M
SW_OPS	Sistemas Operativos	M	1					B	I*, E*, A*	M
HW_BCK	Dispositivos de Respaldo	MA			2		3	M	I*, E*, A*	MA
HW_FRW	Firewall	MA	7					M	I*, E*, A*	MA
HW_HOS	Servidores	MA	5		7	7		M	I*, E*, A*	MA
HW_PCM	Computadoras Portátiles de Uso Institucional	B	1					M	I*, E*, A*	B
HW_PCP	Computadoras de Escritorio de Uso Institucional	B	1					M	I*, E*, A*	B
HW_PRT	Impresoras	MB	1			7		M	I*, E*, A*	MB
HW_ROU	Router	A	1					M	I*, E*, A*	A
HW_SCN	Escáner	MB	5					M	I*, E*, A*	MB
HW_SWH	Switch	A	1			7		M	I*, E*, A*	A
HW_WAP	Puntos de acceso inalámbricos	B	5					M	I*, E*, A*	B
COM_INT	Internet	A	3					A	E*, A*	MA
COM_LAN	Red de Área Local	MA	5					A	E*, A*	MA
COM_WIF	Conectividad Inalámbrica	B	1					A	E*, A*	M
AUX_FBO	Fibra Óptica	MA	5					M	I*, E*, A*	MA
AUX_PWR	Fuente de Alimentación	MA	5					M	I*, E*, A*	MA
AUX_UPS	Fuentes UPS	A	5					M	I*, E*, A*	A
AUX_WIR	Cableado Eléctrico	MA	5					M	I*, E*, A*	MA
L_SIT	Dependencias la unidad educativa	MA	7					MB	N*, I*,E*,A*	A

MA: Muy Alto; A: Alto; M: Medio; B: Bajo; MB: Muy Bajo); Amenazas: [I] De origen industrial; [E] Errores y fallos no intencionados; [A] Ataques intencionados; [N] Desastres naturales; Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad

Tabla generada por el autor a partir de los datos recogidos en el estudio y tras la implementación de la metodología MAGERIT de evaluación de riesgos y amenazas. (CSAE, 2012a).

Anexo 12: Medición del nivel de riesgo detectado en la Unidad Educativa Adventista Gedeón

ACTIVO	AMENAZAS		VULNERABILIDAD	FRECUENCIA O PROBABILIDAD	CRITERIO/ (IMPACTO)	CRITERIO/ (VALOR)	NIVEL DE RIESGO
	TIPO	AMENAZA					
DATOS / INFORMACIÓN	Daño físico	Destrucción de los activos de la información	No existe una planificación de reemplazo de equipos	2	Algunas veces/(3)	Medio/(6)	Normal
		Daño por agentes físicos	Equipos son susceptibles al efecto del polvo y humedad	2	Algunas veces/(1)	Muy Bajo/(2)	Normal
	Eventos naturales	Terremotos	La institución está en área susceptible a efecto de terremotos y erupciones volcánicas	1	Casi nunca/(1)	Muy Bajo/(1)	Normal
	Pérdida de los servicios esenciales	Fallas eléctricas	Instalaciones eléctricas viejas y con cables expuestos en muchas secciones	1	Casi nunca/(4)	Alta/(4)	Normal
		Falla de servicios de internet	Suspensión del servicio u daño de los cables principales de acceso telefónico	3	A menudo/(4)	Alta/(12)	Alta
	Perturbación debido a la radiación	Afección por radiaciones electromagnéticas	Sensibilidad a la radiación electromagnética.	3	A menudo/(2)	Bajo/(6)	Normal
	Compromiso de la información	Robo de documentos físicos	Almacenamiento sin protección.	1	Casi nunca/(4)	Alta/(4)	Normal
		Robo de equipo	Falta de política formal sobre la utilización de computadores portátiles.	4	Casi siempre/(3)	Medio/(12)	Alta
	Fallas técnicas	Fallas técnicas de equipos	Falta de planes de continuidad.	3	A menudo/(4)	Alta/(12)	Alta
		Falta de mantenimiento	Mantenimiento insuficiente.	3	A menudo/(3)	Medio/(9)	Normal
	Acciones no autorizadas	Uso de los equipos sin autorización	Falla en la producción de informes de gestión.	5	Siempre/(5)	Muy alto/(25)	Crítico

		Abuso de derechos y deberes de usuario	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.	5	Siempre/(4)	Alta/(20)	Alta
		Falsificación o usurpación de derechos de acceso	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.	5	Siempre/(4)	Alta/(20)	Alta
SOFTWARE	Daño físico	Destrucción de los activos de la información	No existe una planificación de reemplazo de equipos	1	Casi nunca/(3)	Medio	Normal
		Daño por agentes físicos	Equipos son susceptibles al efecto del polvo y humedad	1	Casi nunca/(1)	Muy Bajo	Normal
	Pérdida de los servicios esenciales	Fallas eléctricas	Computadores y otros equipos sin protección para sobrecargas	5	Siempre/(5)	Medio/(3)	Crítico
	Compromiso con la información	Manipulación inexperta o desautorizada del *software*	Empleo desautorizado de softwares jaqueados	3	A menudo/(3)	Muy Baj/(1)o	Normal
	Acciones no autorizadas	Uso de los equipos sin autorización	Descontrol en el préstamo de equipo	3	A menudo/(3)	Muy alto/(25)	Normal
		Uso ilegal de la información	Creación de cuentas de correo innecesarias	3	A menudo/(4)	Medio/(9)	Alta
	Compromiso de las funciones	Mal uso de los equipos	Falta de directrices de uso	3	A menudo/(3)	Medio/(9)	Normal
		Abuso de derechos y deberes de usuario	Los usuarios no cierran las cesiones o descartan adecuadamente información al terminar las sesiones de trabajo	5	Siempre/(5)	Alta/(12)	Crítico
			En ocasiones se sede a terceros las claves de accesos a alguna computadora que no corresponden a este	5	Siempre/(5)	Medio/(9)	Crítico
		Falsificación o usurpación de derechos de acceso	Muchas computadoras no tienen establecidos métodos de autenticación	5	Siempre/(5)	Muy alto/(25)	Crítico
			Contraseñas inadecuadas y sin recambios	4	Casi siempre/(4)	Muy alto/(25)	Alta

		Fallas logísticas en cuanto a la garantía de mantenimiento	Los equipos no reciben mantenimiento ni de software ni de hardware	3	A menudo/(2)	Muy alto/(25)	Normal
HARDWARE	Daño físico	Destrucción de los activos de la información	No existe una planificación de reemplazo de equipos	2	Algunas veces/(3)	Medio /(6)	Normal
		Daño por agentes físicos	Equipos son susceptibles al efecto del polvo y humedad	1	Casi nunca/(1)	Muy Bajo /(1)	Normal
	Pérdida de los servicios esenciales	Fallas eléctricas	Instalaciones eléctricas viejas y con cables expuestos en muchas secciones	1	Casi nunca/(1)	Muy Bajo/(1)	Normal
		Falla en el equipo de comunicaciones	Suspensión del servicio u daño de los cables principales de acceso telefónico	5	Siempre/(5)	Muy alto/(25)	Crítico
	Compromiso de la información	Manipulación del hardware de los equipos	Acceso a la computadoras sin controles adecuados	5	Siempre/(4)	Alta/(20)	Alta
			Uso indiscriminado de dispositivos extraíbles en los equipos de la institución	5	Siempre/(4)	Alta/(20)	Alta
	Fallas técnicas	Falta de mantenimiento de los equipos	Falta de programas de mantenimiento	3	A menudo/(2)	Bajo/(6)	Normal
		Uso no autorizado de los dispositivos	Falta de controles de acceso a los dispositivos	4	Casi siempre/(3)	Medio/(12)	Alta
	Compromiso de las funciones	Error de uso	Falta de control de cambio con configuración eficiente.	3	A menudo/(3)	Medio/(9)	Normal
		Falsificación de derechos	Falta de mecanismos de identificación y autenticación, como la autenticación de usuario.	5	Siempre/(4)	Alta/(20)	Alta
COMUNICACIONES	Daño físico	Destrucción por accidente o uso de los equipos	Carencia de planes de reemplazo	2	Algunas veces/(2)	Bajo/(4)	Normal
		Daño por agentes físicos	Equipos son susceptibles al efecto del polvo y humedad	1	Casi nunca/(1)	Muy Bajo/(1)	Normal
	Pérdida de los servicios esenciales	Fallas de energía	Equipos sin protección para cambios de tensión	1	Casi nunca/(1)	Muy Bajo/(1)	Normal
		fallas de conexión	Cables de comunicación al alcance de las personas	4	Casi siempre/(4)	Alta/(16)	Alta

	Compromiso de la información	Manipulación no autorizada de software y hardware	Carencia de controles para el uso y acceso a los equipos de computación	4	Casi siempre/(4)	Alta/(16)	Alta
	Fallas técnicas	Fallas del equipos por desactualización	Falta de mantenimiento programado	4	Casi siempre/(4)	Alta/(16)	Alta
		Fallas de equipo por falta de mantenimiento del hardware	Falta de mantenimiento programado	3	A menudo/(2)	Bajo/(6)	Normal
	Acciones no autorizadas	Uso de los equipos sin autorización	Carencia de controles efectivos para control de acceso a los dispositivos	4	Casi siempre/(4)	Alta/(16)	Alta
INSTALACIONES	Eventos naturales	terremotos	Ubicación en una área susceptible de inundación.	4	Casi siempre/(5)	Muy alto/(20)	Alta
	Pérdida de los servicios esenciales	Falta de energía eléctrica	Equipos con posibilidad de sufrir daños por variaciones de tensión	1	Casi nunca/(5)	Muy alto/(5)	Normal
	Acciones no autorizadas	Destrucción de quipos	Falta de rigidez en el control de acceso a las instalaciones y los equipos, así como descontrol en la verificación del uso adecuado de los mismos	4	Casi siempre/(5)	Muy alto/(20)	Alta
	Fallas técnicas	Falta de mantenimiento	Carencia de programas de mantenimiento	1	Casi nunca/(4)	Muy Bajo/(1)	Normal
	Compromiso de las funciones	Indisposición de los servicios	Desconocimiento general del personal sobre, los aspectos asociados a la Seguridad de la gestión de la información	4	Casi siempre/(4)	Alta/(16)	Alta

Tabla diagramada por el Autor.

Anexo 13: Evaluación de cumplimiento de las indicaciones encontradas en el Anexo A.13 de la Norma ISO 27001:2013.

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa		% de cumplimiento
						Si	No	Si	No	
A.5 (políticas de SI)	A.5.1 (Dirección de la gerencia para la SI)	Proporcionar dirección y apoyo de la gerencia para la SI en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes	A.5.1.1	Políticas para la SI	Un conjunto de políticas para la SI debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes	X			X	0%
			A.5.1.2	Revisión de las políticas para la SI	Las políticas para la SI deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua	X			X	
A.6 (organización de la SI)	A.6.1 (Organización Interna)	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la SI dentro de la organización	A.6.1.1	Roles y responsabilidades para la SI	Se debe definir un conjunto de políticas para la SI, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	X			X	0%
			A.6.1.2	Segregación de funciones	Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización	X			X	
			A.6.1.3	Contacto con autoridades	Contactos apropiados con autoridades relevantes deben ser mantenidos.	X			X	
			A.6.1.4	Contacto con grupos especiales de interés	Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos	X			X	
			A.6.1.5	SI en la gestión de proyectos	La SI debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.	X			X	
	A.6.2 (Dispositivos móviles y trabajo a distancia)	Garantizar la seguridad del trabajo a distancia y el uso de dispositivos móviles	A.6.2.1	Políticas de dispositivos móviles	Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.	X			X	
			A.6.2.2	Trabajo a distancia	Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo		X		X	
A.7 (seguridad de los recursos humanos)	A.7.1 (Antes de asumir el empleo)	Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran	A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	x		x		33,3%
			A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la SI	x		x		
	A.7.2 (Durante la ejecución del	Asegurarse de los empleados y contratistas	A.7.2.1	Responsabilidades de la gerencia	La gerencia debe requerir a todos los empleados y contratistas aplicar la SI en concordancia con las políticas y procedimientos establecidos por la organización.	x			x	

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa		% de cumplimiento
						Si	No	Si	No	
		tomen conciencia de sus responsabilidades de SI y las cumplan	A.7.2.2	Conciencia, educación y capacitación sobre la SI	Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la SI, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	x			x	
			A.7.2.3	Proceso Disciplinarios	Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la SI.	X			X	
	A.7.3 (Terminación y cambio de empleo)	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y deberes de SI que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.	X			X	
A.8 (gestión de activos)	A.8.1 (Responsabilidad por los activos)	Identificar los activos organizacionales y definir las responsabilidades apropiadas	A.8.1.1	Inventario de activos	Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.	X			X	20%
			A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben ser propios	X		X		
			A.8.1.3	Uso aceptable de los activos	Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas	X			X	
			A.8.1.4	Retorno de activos	Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo	X		X		
	A.8.2 (Clasificación de la Información)	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo a su importancia para la organización	A.8.2.1	Clasificación de la Información	La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	X			X	
			A.8.2.2	Etiquetado de la información	Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización	X			X	
			A.8.2.3	Manejo de activos	Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	X			X	
	A.8.3 (Manejo de medios)	Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios	A.8.3.1	Gestión de medios removibles	Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	X			X	
			A.8.3.2	Disposición de medios	Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales	X			X	
			A.8.3.3	Transferencia de medios físicos	Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte	X			X	

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa		% de cumplimiento
						Si	No	Si	No	
A.9 (control de acceso)	A.9.1 (Requisitos del negocio para control de acceso)	Limitar el acceso a información y a instalaciones de procesamiento de información	A.9.1.1	Política de control de acceso	Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de SI	X			X	
			A.9.1.2	Acceso a redes y a servicios de red	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	X			X	
	A.9.2 (Gestión de acceso de usuarios)	Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios	A.9.2.1	Registro y baja de usuarios	Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.	X			X	
			A.9.2.2	Aprovisionamiento de acceso a usuario	Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.		X	X		
			A.9.2.3	Gestión de los derechos de acceso privilegiado	La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada	X		X		
			A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal	X		X		
			A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares	X			X	
			A.9.2.6	Remoción o ajuste de derechos de acceso	Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.	X			X	57,14%
	A.9.3 (Responsabilidades de los usuarios)	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación	A.9.3.1	Uso de información de autenticación secreta	Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta	X		X		
	A.9.4 (Responsabilidades de los usuarios)	Evitar el acceso no autorizado a sistemas y aplicaciones	A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso	X		X		
			A.9.4.2	Procedimiento de ingreso seguro	Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro	X		X		
			A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas	X			X	
			A.9.4.4	Uso de programas utilitarios privilegiados	El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente	X		X		
			A.9.4.5	Control de acceso a códigos fuente de los programas	El acceso al código fuente de los programas debe ser restringido	X		X		
A.10. (Criptog	A.10.1 (Controles Cript	Asegurar el uso apropiado y	A.10.1.1	Política sobre el uso de controles criptográficos	Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	X			X	0%

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa		% de cumplimiento
						Si	No	Si	No	
		eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información	A.10.1.2	Gestión de claves	Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.		X		X	
A.11 (Seguridad física y del entorno)	A.11.1 (Áreas seguras)	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización	A.11.1.1	Perímetro de seguridad física	Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información	X		X		
			A.11.1.2	Controles de ingreso físicos	Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado	X		X		
			A.11.1.3	Asegurar oficinas, áreas e instalaciones	Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada	X		X		
			A.11.1.4	Protección contra amenazas externas y ambientales	Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	X			X	
			A.11.1.5	Trabajo en áreas seguras	Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado		X		X	
			A.11.1.6	Áreas de despacho y carga	Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.		X		X	
	A.11.2 (Equipos)	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización	A.11.2.1	Emplazamiento y protección de los equipos	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado	X		X		41,6%
			A.11.2.2	Servicios de suministro	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro	X			X	
			A.11.2.3	Seguridad del cableado	El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño	X			X	
			A.11.2.4	Mantenimiento de equipos	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad	X			X	
			A.11.2.5	Remoción de activos	Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.	X		X		
			A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.		X		X	
			A.11.2.7	Disposición o reutilización segura de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización	X			X	

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa		% de cumplimiento
						Si	No	Si	No	
			A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que los equipos desatendidos tenga la protección apropiada	X			X	
			A.11.2.9	Políticas de escritorio limpio y pantalla limpia	Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada	X			X	
A.12 (Seguridad de las operaciones)	A.12.1 (Procedimientos operacionales y responsabilidades)	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de Información	A.12.1.1	Procedimientos de operativos documentados	Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan	X			X	38,46%
			A.12.1.2	Gestión de Cambios	Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la SI deben ser controlados.	X		X		
			A.12.1.3	Gestión de Capacidad	El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	X		X		
			A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.		X		X	
	A.12.2 (Protección contra códigos maliciosos)	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos	A.12.2.1	Controles contra códigos maliciosos	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios	X		X		
	A.12.3 (Respaldo)	Proteger contra la pérdida de datos	A.12.3.1	Respaldo de la información	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	X		X		
	A.12.4 (Copias de respaldo)	Registrar eventos y generar evidencia	A.12.4.1	Registro de eventos	Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de SI deben ser producidos, mantenidos y regularmente revisados.	X			X	
			A.12.4.2	Protección de información de registro	Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	X			X	
			A.12.4.3	Registros del administrado y del operador	Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente	X			X	
			A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.	X		X		

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa		% de cumplimiento
						Si	No	Si	No	
	A.12.5 (Control de *software* operacional)	Asegurarse de la integridad de los sistemas operacionales	A.12.5.1	Instalación de *software* en sistemas operacionales	Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales	X			X	
	A.12.6 (Gestión de la vulnerabilidad técnica)	Prevenir el aprovechamiento de las vulnerabilidades técnicas	A.12.6.1	Gestión de las vulnerabilidades técnicas	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado	X			X	
			A.12.6.2	Restricciones sobre la instalación de *software*	Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	X			X	
	A.12.7 (Consideraciones sobre auditorías de sistemas de	Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos	A.12.7.1	Controles de auditorías de sistemas de información	Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.	X			X	
A.13 (Seguridad de las comunicaciones)	A.13.1 (Gestión de seguridad de la red Objetivo: Asegurar la protección	Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo	A.13.1.1	Controles de redes	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones	X			X	
			A.13.1.2	Seguridad de los servicios de red	Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	X			X	
			A.13.1.3	Segregación de redes	Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.		x		x	
	A.13.2 (Transferencia de información)	Mantener la SI transferida dentro de una organización y con cualquier entidad externa	A.13.2.1	Políticas y procedimientos de transferencia de información	Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	X		X		33,3%
			A.13.2.2	Acuerdos sobre la transferencia de información	Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas	X			X	
			A.13.2.3	Mensajería electrónica	La información involucrada en mensajería electrónica debe ser protegida apropiadamente	X			X	
			A.13.2.4	Acuerdos de confidencialidad o no divulgación	Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados	X		X		
A.14 (Adquisición, desarrollo y	A.14.1 (Requisitos de seguridad de los sistemas de información)	Asegurar que la SI sea una parte integral de los sistemas de información durante todo el	A.14.1.1	Análisis y especificación de requisitos de SI	Requisitos relacionados a la SI deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes	X			X	25%
			A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.	X			X	

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa	% de cumplimiento
						Si	No	Si	No
		ciclo de vida. Esto incluye los requisitos para sistemas de información que presten servicios sobre redes públicas	A.14.1.3	Protección de transacciones de los servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.	X			X
	A.14.2 (Seguridad en los procesos de desarrollo y soporte)	Asegurar que la SI esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	A.14.2.1	Política de desarrollo seguro	Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.		X		X
			A.14.2.2	Procedimientos de control de cambio del sistema	Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.		X		X
			A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.		X		X
			A.14.2.4	Restricciones sobre cambios a los paquetes de *software*	Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.		X		X
			A.14.2.5	Principios de ingeniería de sistemas seguros	Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información		X		X
			A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.		X		X
			A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.	X		X	
			A.14.2.8	Pruebas de seguridad de sistemas	Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.		X		X
			A.14.2.9	Pruebas de aceptación de sistemas	Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.		X		X
	A.14.3 (Datos de prueba)	Asegurar la protección de los datos usados para pruebas	A.14.3.1	Protección de datos de prueba	Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.		X		X
A.15 (Relaciones	A.15.1 (SI en las relaciones con	Asegurar la protección de los activos de la	A.15.1.1	Política de SI para las relaciones con los proveedores	Requisitos de SI para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.	x			x	0%

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa	% de cumplimiento
						Si	No	Si	No
		organización que sean accesibles a los proveedores	A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Todos los requisitos relevantes de SI deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.	x			X	
			A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de SI asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	X			x	
	A.15.2 (Gestión de la prestación de servicios de proveedores)	Mantener un nivel de SI y entrega de servicios acordado en línea con los acuerdos con proveedores	A.15.2.1	Monitoreo y revisión de servicios de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores	X			X	
			A.15.2.2	Gestión de cambios en los servicios de los proveedores	Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de SI deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	X			X	
A.16 (Gestión de incidentes de SI)	A.16.1 (Gestión de incidentes de SI y mejoras)	Asegurar un enfoque consistente y efectivo a la gestión de incidentes de SI, incluyendo la comunicación sobre eventos de seguridad y debilidades	A.16.1.1	Responsabilidades y procedimientos	Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de SI.	X			X	
			A.16.1.2	Reporte de eventos de SI	Los eventos de SI deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible	X		X		
			A.16.1.3	Reporte de debilidades de SI	Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a SI en los sistemas o servicios.	X			X	
			A.16.1.4	Evaluación y decisión sobre eventos de SI	Los eventos de SI deben ser evaluados y debe decidirse si son clasificados como incidentes de SI	X			X	14,28%
			A.16.1.5	Respuesta a incidentes de SI	Los incidentes de SI deben ser respondidos de acuerdo con los procedimientos documentados	X			X	
			A.16.1.6	Aprendizaje obtenido de los incidentes de SI	El conocimiento adquirido a partir de analizar y resolver los incidentes de SI debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros	X			X	
			A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	X			X	
A.17 (Aspectos de SI de la gestión de	A.17.1 (Continuidad de SI)	La continuidad de SI debe estar embebida en los sistemas de gestión de continuidad del	A.17.1.1	Planificación de la continuidad de la SI	La organización debe determinar sus requisitos de SI y continuidad de la gestión de SI en situaciones adversas, por ejemplo durante una crisis o desastre.	X			X	0%
			A.17.1.2	Implementación de la continuidad de la SI	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la SI durante una situación adversa.	X			X	

Anexo	Sub punto	Objetivo	Apartado	Requisito	Control	Aplica		Implementa		% de cumplimiento
						Si	No	Si	No	
		negocio de la organización	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la SI	La organización debe verificar los controles de continuidad de SI que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	X			X	
	A.17.2 (Redundancias)	Asegurar la disponibilidad de instalaciones de procesamiento de información.	A.17.2.1	Instalaciones de procesamiento de la información	Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	X			X	
A.18 (Cumplimiento)	A.18.1 (Cumplimiento de los requisitos legales y contractuales)	Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la SI y a cualquier requisito de seguridad.	A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.	X		X		
			A.18.1.2	Derechos de propiedad intelectual	Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.		X		X	
			A.18.1.3	Protección de registros	Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	X			X	
			A.18.1.4	Privacidad y protección de información de datos personales	La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	X		X		28,57%
			A.18.1.5	Regulación de controles criptográficos	Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes	X			X	
	A.18.2 (Revisiones de SI)	Asegurar que la SI está implementada y es operada de acuerdo con las políticas y procedimientos organizativos	A.18.2.1	Revisión independiente de la SI	El enfoque de la organización para manejar la SI y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la SI) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.	X			X	
			A.18.2.2	Cumplimiento de políticas y normas de seguridad	Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	X			X	
			A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información deben ser revisados regularmente respecto a cumplimiento de las políticas y normas de SI de la organización.	X			X	
Total Promedio de cumplimiento										20,83%

Diagramado por el Autor. Referencia: ISO 27001:2013 (2014).

Anexo 14: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE SI.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

OBJETIVO, ALCANCE Y USUARIOS

El propósito de esta Política es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

L misma se aplica a todo el SGSI, según se define en el manual, particularmente en la sección de Alcance. Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón, así como también terceros externos a la misma.

1. Documentos de referencia:

- Norma ISO 27001:2013, clausulas 5.2 y 6.2
- Manual del SGSI
- Metodología de evaluación y tratamiento de riesgos empleada (MAGERIT, en sus libros 1, 2 y 3)
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales
- Política de la Continuidad del Negocio
- Procedimiento para gestión de incidentes

2. Terminología empleada:

Confidencialidad: Característica de la información que indica que esta solo se encuentra disponible solo para personas o sistemas autorizados.

Integridad: Característica de la información que indica que esta solo es modificada por personas o sistemas autorizados.

Disponibilidad: Característica de la información, la cual hace referencia a que esta solo puede accederse por parte de personas autorizadas cuando sea necesario.

Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 15: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA ACERCA DE DISPOSITIVOS MÓVILES.

	POLÍTICA ACERCA DE DISPOSITIVOS MÓVILES	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es evitar el acceso no autorizado a dispositivos ubicados tanto dentro como fuera de las instalaciones de la Unidad Educativa Gedeón. Este documento se aplica a todo el alcance del SGSI; es decir, a todas las personas, datos y equipos incluidos en el alcance del mismo.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia:
   - Norma ISO 27001, clausulas A.6.2 y A.11.2.6
   - Política de Seguridad de la Información
   - Política de Clasificación de la Información
   - Política de uso aceptable

3. Equipos móviles de computación

3.1. Introducción

Entre los equipos de computación móviles, se incluyen las portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

El equipamiento mencionado anteriormente únicamente puede ser transportado fuera de las instalaciones con la debida autorización de la dirección de la Unidad

Educativa Gedeón, previa firma de un acta de compromiso en la que se indique el compromiso de garantizar la confidencialidad de la información contenida en ellos.

La seguridad aplicable a estos dispositivos es semejante a la empleada dentro de las instalaciones de la institución y se deben emplear los siguientes controles adicionales con el fin de aminorar los riesgos que por sí mismo conlleva el empleo de estos, así:

- Los equipos móviles institucionales, no pueden conectarse a redes inalámbricas públicas o no conocidas.
- El software instalado en los dispositivos móviles debe ser licenciado y solo debe ser realizado por parte del personal técnico autorizado para tal fin, el cual debe llevar un reporte individual para cada equipo de cada una de estas acciones.
- El acceso a los equipos móviles se realiza mediante el uso de usuario y contraseñas, misma que no puede ser cambiada más que en presencia del personal técnico autorizado, el cual, generará un reporte con la fecha de dicha modificación de acceso.
- La información almacenada en los equipos de portátiles, debe ser cifrada, y debe ser respalda en otros medios por parte del personal técnico autorizado en periodos regulares y programados de tiempo.
- Se debe realizar borrado seguro de la información o destrucción física del dispositivo de almacenamiento (si se encuentra dañado y sin posibilidades de ser reparado sin que genere un riesgo de pérdida de información para la institución, este proceso debe ser documentado y justificado), después de ser entregado por algún empleado que deje de pertenecer a la institución y antes de ser reasignado.
- Se debe realizar verificaciones periódicas para comprobar el retiro no autorizado de activos.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 16: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN.

	POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es el de garantizar que se proteja la información a un nivel conveniente.

Este documento se aplica a todo el alcance del SGSI; es decir, a todos los tipos de información, indistintamente del formato (papel o digital), aplicaciones y bases de datos, conocimiento de las personas.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia:

- Norma ISO 27001, clausulas: A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- Política de Seguridad de la Información
- Informe de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Inventario de activos
- Lista de obligaciones legales, normativas y contractuales
- Procedimiento para gestión de incidentes
- Procedimientos operativos para tecnología de la información y de la comunicación/Política de eliminación y destrucción
- Política de Uso aceptable

3. Información clasificada:

3.1. Pasos y responsabilidades

Los pasos y responsabilidades para la gestión de la información son los siguientes:

No.	Nombre del paso	Responsabilidad
1	**Ingreso del activo de información en el Inventario de activos**	[Definir responsable]
2	**Clasificación de la información**	Propietario del activo
3	**Etiquetado de la información**	Propietario del activo
4	**Manejo de la información**	Personas que poseen derechos de acceso de acuerdo con esta Política

Si la información es generada de manera externa a la unidad educativa, el responsable del ingreso a la institución de la misma es el garante de su clasificación en base a las directrices indicadas en la presente Política, y esta persona termina siendo el señalado como el propietario de esa información.

3.2. Clasificación de la información

La información se clasifica según los preceptos de confidencialidad, integridad y disponibilidad:

3.2.1. Clasificación según su confidencialidad

La información se clasificará de la siguiente manera:

- **PRIVADA**: información cuya divulgación no autorizada puede ser perjudicial para los intereses de la Institución o de uno, varios o todos los miembros de los distintos Stakeholders.
- **RESERVADA**: información que debe ser conocida por los empleados para el desarrollo adecuado de sus actividades.
- **PUBLICA**: información que no representa riesgo para ninguna de las partes interesadas y que puede ser divulgada sin problemas evidentes.

3.2.2. Clasificación según su integridad

La información se clasificará de la siguiente manera:

Nivel 4.: No puede ser reparado o manipulada, y la misma, ocasiona pérdidas graves para la institución.

Nivel 3.: Elemento de difícil reparación y produce pérdidas significativas.

Nivel 2.: Puede repararse, produce pérdidas leves.

Nivel 1.: No afecta la operación y puede repararse fácilmente.

3.2.23. Clasificación Según su disponibilidad

La información se clasificará según su disponibilidad de la siguiente manera:

Es necesario determinar el tiempo máximo tolerable que puede soportar la unidad educativa sin un activo determinado, para lo cual, se tendrá en cuenta la siguiente clasificación:

Nivel 5.: CRÍTICOS, la interrupción es de minutos y hasta 12 horas.

Nivel 4.: URGENTE, la interrupción hasta por 24 horas.

Nivel 3. IMPORTANTE, interrupción hasta por 72 horas.

Nivel 2.: NORMAL, interrupción de hasta siete días

Nivel 1.: NO ESENCIALES, la interrupción es de hasta 30 días

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 17: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE USO ACEPTABLE.

	POLÍTICA DE USO ACEPTABLE	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir las reglas para el uso de los sistemas y de otros activos de información de la Unidad Educativa Gedeón.

Este documento se aplica a todo el alcance del SGSI; es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del sistema de gestion.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia

- Norma ISO 27001, clausulas A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
- Política de Seguridad de la Información
- Política de Clasificación de la Información
- Procedimiento para gestión de incidentes
- Inventario de activos
- Procedimientos operativos para tecnología de la información y de la comunicación
- Política de Transferencia de la Información

3. Uso aceptable de los activos de información

3.1. Definiciones

Sistema de información: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes

que pertenecen o son utilizados por la institución, o que se encuentran bajo su responsabilidad. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

Activos de información: en el contexto de esta Política, el término se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, computadores portátiles, soportes de almacenamiento de datos, entre otros.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 18: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE CLAVES.

	POLÍTICA DE CLAVES	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es establecer reglas para garantizar la gestión y utilización seguras de las claves.

Este documento se aplica a todo el alcance del SGSI; es decir, a todos los puestos de trabajo y sistemas ubicados dentro del alcance del sistema.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia

- Norma ISO 27001, clausulas A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
- Política de Seguridad de la Información
- Declaración de aceptación de los documentos del sistema de gestión

3. Obligaciones de los usuarios

- Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves
- La asignación de claves de acceso a equipos y a la red debe ser realizada y documentada por el técnico a cargo, previa solicitud por escrito.
- Nadie puede modificar o cambiar las claves de acceso a los dispositivos y a las redes sin que esta quede documentada por el personal técnico a cargo.
- No se puede asignar o prestar claves de acceso a dispositivos o redes sin que esto sea una violación grave de las políticas del SGSI y que no sea autorizado de manera expresa por la dirección del sistema de gestión.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 19: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE CONTROL DE ACCESO.

	POLÍTICA DE CONTROL DE ACCESO	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad.

Este documento se aplica a todo el alcance del SGSI; es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del sistema de gestión. Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia

- Norma ISO 27001, clausulas A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3
- Política de Seguridad de la Información
- Declaración de aplicabilidad
- Política de Clasificación de la Información
- Declaración de aceptación de los documentos del SGSI
- Lista de requisitos legales, normativos, contractuales y de otra índole

3. Control de acceso

3.1. Introducción

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios. Debe existir un procedimiento de registro de usuarios para cada sistema y servicio.

Está permitido el acceso a todos los sectores físicos de la institución excepto a aquellos para las cuales el privilegio debe ser concedido por una persona autorizada.

Esta Política determina.

Todo empleado de la institución con acceso a Internet a través del servicio contratado por la institución, tiene restringido el uso de:

- Mensajería instantánea comercial.
- Uso de telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Servicios de escritorio remoto a través de internet.
- Acceso a redes sociales
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 20: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE ELIMINACIÓN Y DESTRUCCIÓN.

	POLÍTICA DE ELIMINACIÓN Y DESTRUCCIÓN	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar que la información almacenada en equipos y soportes sea borrada o eliminada de forma segura.

Este documento se aplica a todo el alcance del SGSI; es decir, a toda la tecnología de la información y de la comunicación, como también a la documentación dentro del alcance del sistema de gestión.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón

2. Documentos de referencia

- Norma ISO 27001, clausulas A.8.3.2, A.11.2.7
- Política de Seguridad de la Información
- Política de Clasificación de la Información
- Inventario de activos

3. Eliminación y destrucción de equipos y soportes

Todos los datos y software con licencia almacenados en soportes móviles, es decir, CD, DVD, dispositivos de memoria extraíble, otras tarjetas de memoria, discos duros, papel, sin limitarse solo a los mencionados, así como, a todos los equipos que tienen soportes de almacenaje entre los que se encuentran (no limitándose solo a estos) computadores tanto de mesa como portátiles, teléfonos móviles, y tabletas, deben ser borrados, o se debe destruir el soporte, antes de su devolución o reutilización.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 21: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIOS.

	POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIOS	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos.

Este documento se aplica a todo el alcance del SGSI; es decir, a todos los puestos de trabajo, instalaciones y equipos ubicados dentro del alcance del sistema de gestión.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia

- Norma ISO 27001, clausulas A.11.2.8 y A.11.2.9
- Política de Seguridad de la Información
- Política de Clasificación de la Información

3. Política de pantalla y escritorio limpio

Toda la información clasificada como "Uso interno", "Restringido" y "Confidencial" de acuerdo a lo establecido en la Política de Clasificación de la Información, es considerada sensible en esta Política de pantalla y escritorio limpio.

3.1. Protección del puesto de trabajo

3.1.1. Política de escritorio limpio

- Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos deben estar almacenados en sitios seguros bajo llave, especialmente si la persona se encuentra fuera de su horario laboral.
- Cuando el empleado no se encuentre utilizando el computador, debe bloquearse la sesión, el protector de pantalla se debe activar automáticamente después de cinco (5) minutos de inactividad.
- Cuando se imprima información considerada como sensible no se debe dejar disponible, debe ser almacenada inmediatamente.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 22: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLITICAS PARA TRABAJO EN ÁREAS SEGURAS.

	POLITICAS PARA TRABAJO EN ÁREAS SEGURAS	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir las reglas básicas de comportamiento en las áreas seguras. Este documento se aplica a todas las áreas seguras SGSI.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia

- Norma ISO 27001, clausulas A.11.1.5
- Política de control de acceso
- Inventario de activos

3. Reglas para áreas seguras

3.1. Lista de áreas seguras

Las áreas seguras existentes que requieren reglas especiales son las siguientes:

- Aula de computación
- Sala de archivos
- Oficinas administrativas
- Sala de almacenamiento de equipos

Las personas responsables para cada área segura se detallan como propietarios de activos en el Inventario de activos.

3.2. Derecho de acceso a áreas seguras

- El acceso a las áreas seguras se autoriza de acuerdo con la Política de control de acceso.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 23: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN.

	POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es asegurar la seguridad de la información y el software cuando son intercambiados dentro o fuera de la organización. Este documento se aplica a todo el alcance del SGSI; es decir, a toda la información y tecnología de la información y de la comunicación utilizada dentro del alcance del sistema de gestión.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia

- Norma ISO 27001, puntos A.13.2.1, A.13.2.2
- Política de Seguridad de la Información
- Política de Clasificación de la Información
- Política de seguridad para proveedores

3. Transferencia de la información

3.1. Canales de comunicación electrónica

La información de la organización puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, descarga de archivos desde Internet, transferencia de datos por medio de Dropbox, teléfonos, equipos de fax, mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

3.2. Registro de incidentes

Los incidentes tales como: fallas humanas (voluntarias e involuntarias), ataques informáticos, errores del sistema, desastres naturales, fallas de sistemas de alimentación, se clasifican dentro de los siguientes tipos:

- Relacionados con la información (directamente relacionados con tecnología de la información y comunicación)
- No relacionados con la información (todos los demás incidentes)

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

Anexo 24: Documentación asociada a las políticas de seguridad del manual del SGSI propuesto: POLÍTICA PARA GESTIÓN DE INCIDENTES DE SEGURIDAD.

	POLÍTICA PARA GESTIÓN DE INCIDENTES DE SEGURIDAD	Código	
		Versión:	0.1
		Fecha de la versión	
		Creado por:	
		Aprobado por:	Junta directiva
		Nivel de confidencialidad:	Alto

1. Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta ante incidentes de seguridad. Este documento se aplica a todo el alcance del SGSI; es decir, a todos los empleados y demás activos que se utilizan dentro del alcance del sistema de gestión, como también a los proveedores y demás personas externas a la organización que entran en contacto con los sistemas y con la información alcanzados por el sistema.

Los usuarios de este documento son todos los empleados de la Unidad Educativa Gedeón.

2. Documentos de referencia

- Norma ISO 27001, clausulas A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
- Política de Seguridad de la Información
- Lista de requisitos legales, normativos, contractuales y de otra índole

3. Gestión de incidentes

Un incidente de seguridad de la información es un "*evento, o serie de eventos, indeseado e inesperado que tiene una alta probabilidad de poner en riesgo las actividades comerciales y de amenazar la seguridad de la información*" (ISO/IEC 27000:2009).

3.1. Recepción y clasificación de incidentes, debilidades y eventos

Cada empleado, proveedor o tercero que esté en contacto con información y/o sistemas de información debe reportar de la siguiente manera toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente:

- Reportar los eventos de seguridad siguiendo los procedimientos operativos establecidos para tal fin.
- Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática que afecte a activos de información considerado como crítico.
- Ejecutar acciones tendientes a reducir y mitigar el incidente.
- Asimilar de las experiencias tenidas ende los incidentes de seguridad de la información, para aprender a prevenir nuevas ocurrencias.
- Subsanar las consecuencias de los incidentes de seguridad de la información.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1		Descripción básica del documento

EDUCACIÓN
ADVENTISTA

UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

APROBACIÓN

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

A través del presente documento se hace la constancia de la aprobación de un Sistema de Gestión de Seguridad de la Información para la Unidad Educativa Adventista Gedeón, el cual permitirá conocer los diferentes tipos de activos para su etiquetado, análisis, evaluación y tratamiento de riesgos con la finalidad de proteger los recursos tecnológicos y de información.

Quito D. M., 29 de enero de 2019

UNIDAD EDUCATIVA "ADVENTISTA GEDEON" RECTORADO

Mg. Paulina Mulki
Directora Unidad Educativa Adventista Gedeón
UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

EDUCACIÓN
ADVENTISTA

UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

APROBACIÓN

INVENTARIO DE ACTIVOS

DECLARACIÓN

A través del presente documento se hace la constancia de la aprobación sobre la realización del Inventario de Activos para la Unidad Educativa Adventista Gedeón, el cual permitirá conocer y clasificar cada uno de ellos de mejor manera para su gestión.

Quito D. M., 29 de enero de 2019

Mg. Paulina Mulki
Directora Unidad Educativa Adventista Gedeón
UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

UNIDAD EDUCATIVA "ADVENTISTA GEDEON"
RECTORADO
QUITO - ECUADOR

EDUCACIÓN
ADVENTISTA

UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

APROBACIÓN

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

DECLARACIÓN

A través del presente documento se hace la constancia de la aprobación de la Metodología de Evaluación y Tratamiento de Riesgos para la Unidad Educativa Adventista Gedeón, el cual permitirá realizar un análisis de los activos sobre las amenazas a las que están expuestas identificando las vulnerabilidades y el impacto que éstas tendrían a través de los resultados obtenidos.

Quito D. M., 20 de febrero de 2019

UNIDAD EDUCATIVA "ADVENTISTA GEDEON" RECTORADO QUITO - ECUADOR

Mg. Paulina Mulki
Directora Unidad Educativa Adventista Gedeón
UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

EDUCACIÓN
ADVENTISTA

UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

APROBACIÓN

DECLARACIÓN DE APLICABILIDAD

DECLARACIÓN

A través del presente documento se hace la constancia de la aprobación de la Declaración de Aplicabilidad para la Unidad Educativa Adventista Gedeón, el cual permite sugerir los controles que son aplicables basándose en los resultados de la evaluación de riesgos realizada.

Quito D. M., 22 de marzo de 2019

Mg. Paulina Mulki
Directora Unidad Educativa Adventista Gedeón
UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

UNIDAD EDUCATIVA "ADVENTISTA GEDEON"
RECTORADO
ARMENIA - ECUADOR

EDUCACIÓN
ADVENTISTA

UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

APROBACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

A través del presente documento se hace la constancia de la aprobación de la elaboración de Políticas de Seguridad de la Información para la Unidad Educativa Adventista Gedeón, las cuales permitirán documentar, registrar y utilizar para las diferentes actividades académicas, en las que dichas políticas deberán ser comunicadas al personal para su cumplimiento y seguimiento.

Quito D. M., 26 de julio de 2019

Mg. Paulina Mulki
Directora Unidad Educativa Adventista Gedeón
UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

UNIDAD EDUCATIVA "ADVENTISTA GEDEON"
RECTORADO
ARMENIA - ECUADOR

EDUCACIÓN
ADVENTISTA

UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

APROBACIÓN

FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN

A través del presente documento se hace la constancia de la aprobación de la definición de Funciones y Responsabilidades de Seguridad de la Información para la Unidad Educativa Adventista Gedeón, las cuales se deben puntualizar acerca de quiénes serán los responsables de proteger y velar por la seguridad de la información tanto de los recursos tecnológicos como lo de la información.

Quito D. M., 26 de julio de 2019

Mg. Paulina Mulki
Directora Unidad Educativa Adventista Gedeón
UNIDAD EDUCATIVA ADVENTISTA GEDEÓN

UNIDAD EDUCATIVA "ADVENTISTA GEDEON" DIRECTORADO ECUADOR